

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

#2
S&H Form: (2/01)

Attorney Docket No. 1075.1166



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Takashi SHINZAKI

Application No.:

Group Art Unit:

Filed: May 22, 2001

Examiner:

For: PUBLICATION CERTIFYING SYSTEM, VIEWING-ACCESS-LOG RECORDING
SERVER, PUBLISHING-ACCESS-LOG RECORDING SERVER, DIGITAL-SIGNATURE
SERVER, AND INFORMATION TERMINAL FOR ACCESS-TO-VIEW

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith
a certified copy of the following foreign application:

Japanese Patent Application No. 2000-368514

Filed: December 4, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing
date(s) as evidenced by the certified papers attached hereto, in accordance with the
requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 5/22/01

By: 

James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

©2001 Staas & Halsey LLP

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

J1033 U.S. PTO
09/862433
05/23/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2000年12月 4日

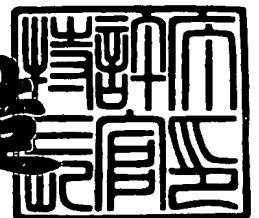
出願番号
Application Number: 特願2000-368514

出願人
Applicant(s): 富士通株式会社

2001年 3月 2日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3014918

【書類名】 特許願

【整理番号】 0052178

【提出日】 平成12年12月 4日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 19/00

【発明の名称】 公開立証システム並びに閲覧アクセスログ記録サーバ、
掲載アクセスログ記録サーバおよびデジタル署名サーバ
並びに閲覧アクセス用情報端末

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通
株式会社内

【氏名】 新崎 卓

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100092978

【弁理士】

【氏名又は名称】 真田 有

【電話番号】 0422-21-4222

【手数料の表示】

【予納台帳番号】 007696

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704824

特 2 0 0 0 - 3 6 8 5 1 4

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 公開立証システム並びに閲覧アクセスログ記録サーバ、掲載アクセスログ記録サーバおよびデジタル署名サーバ並びに閲覧アクセス用情報端末

【特許請求の範囲】

【請求項 1】 提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報揭示機能とを有する情報提供サーバと、

該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとをそなえたことを特徴とする、公開立証システム。

【請求項 2】 通信ネットワークを介して閲覧された公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有することを特徴とする、閲覧アクセスログ記録サーバ。

【請求項 3】 通信ネットワークを介して情報提供サーバに送信・掲載された公開情報と該公開情報の掲載日時とを掲載アクセスログとして獲得する掲載アクセスログ獲得機能と、該掲載アクセスログ獲得機能によって獲得された該掲載アクセスログを保存する掲載アクセスログ保存機能とを有することを特徴とする、掲載アクセスログ記録サーバ。

【請求項 4】 提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報揭示機能とを有する情報提供サーバと、

該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開

情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとともに公開立証システムを構成するデジタル署名サーバであって、

該閲覧アクセスログにタイムスタンプを付加するタイムスタンプ付加機能と、該タイムスタンプを付加された該閲覧アクセスログを、該デジタル署名サーバの秘密鍵を用いて暗号化することにより、該タイムスタンプ付き閲覧アクセスログにデジタル署名を施す暗号化機能とを有することを特徴とする、デジタル署名サーバ。

【請求項 5】 提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報揭示機能とを有する情報提供サーバと、

該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとともに公開立証システムを構成する情報端末であって、

該閲覧アクセスログ記録サーバにおいて該公開情報に対する閲覧アクセスログを意図的に残すことを目的として、該情報提供サーバにおける該公開情報に対する閲覧アクセスを定期的に行なうことを特徴とする、閲覧アクセス用情報端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、電子データが通信ネットワーク上で第三者が閲覧・アクセス可能な状態で保管されていたこと、即ち、電子データが通信ネットワーク上で第三者に対して公開されていたことを立証するための、公開立証システム並びに閲覧アクセスログ記録サーバ、掲載アクセスログ記録サーバおよびデジタル署名サーバ並びに閲覧アクセス用情報端末に関し、例えば、企業からの各種情報（例えばリコ

ールに伴う製品障害情報，製品回収情報等）が電子データとして通信ネットワーク上で掲示・公開されていたことや、各種技術情報が電子データとして通信ネットワーク上で公開されて公知化されていることを証明する手段（サービス）として広く活用されうるものである。

【 0 0 0 2 】

【従来の技術】

近年、紙等の印刷物によって情報の開示を行なう代わりに、その情報をインターネット〔例えばWWW（World Wide Web）〕上で電子データとして掲示・公開することが一般的になっている。

より具体的に説明すると、情報掲載希望者は、例えばパソコン等の情報端末からインターネットを介して情報提供サーバにアクセスし、掲載希望情報を情報提供サーバに送信し、その情報を情報提供において電子データとして外部からアクセス可能な状態で保管させる。これにより、第三者は、パソコン等の情報端末からインターネットを介して情報提供サーバにアクセスすれば、その情報提供サーバに保管された電子データを閲覧することができるようになっている。

【 0 0 0 3 】

【発明が解決しようとする課題】

ところで、近年、電子データがいつ作成されたかを立証するために、公開鍵暗号化技術やメッセージダイジェスト作成技術を組み合わせたデジタル署名技術が用いられ始めている。

しかし、特許審査等に際しての公知例範囲にインターネット上での公開情報を含める場合や、企業がWWW上で例えばリコールに伴う製品障害情報，製品回収情報等の告知を行なう場合、その情報としての電子データの作成日時を立証するだけでなく、その電子データが第三者からのアクセスが容易な場所（サーバ）で掲示・公開されていたことや、その電子データが掲示・公開されていた期間を立証することが必要になる。

【 0 0 0 4 】

例えば、雑誌等については国立国会図書館でそのほとんどを保管されているため、その情報の公開を立証することが比較的容易であるが、電子データが通信ネ

ットワーク上において第三者が閲覧可能な状態で掲示・公開されていた日時（期間）を立証することには困難が伴っている。このため、現状では、電子データの通信ネットワーク上での公開を立証するための手法やシステムは確立されておらず、その手法やシステムの開発が強く望まれている。

【0005】

本発明は、このような要望に鑑み創案されたもので、各種情報が電子データとして通信ネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを立証できるようにして、その通信ネットワーク上で掲示・公開された情報にも、印刷物や出版物と同様の証拠能力をもたせることを実現した、公開立証システム並びに閲覧アクセスログ記録サーバ、掲載アクセスログ記録サーバおよびデジタル署名サーバ並びに閲覧アクセス用情報端末を提供することを目的とする。

【0006】

【課題を解決するための手段】

上記目的を達成するために、本発明の公開立証システム（請求項1）は、提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報掲示機能とを有する情報提供サーバと、該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとをそなえたことを特徴としている。

【0007】

また、本発明の閲覧アクセスログ記録サーバ（請求項2）は、通信ネットワークを介して閲覧された公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有することを特徴としている。

【 0 0 0 8 】

上述の構成により、第三者が、情報提供サーバに保存されている公開情報を閲覧すべく、情報端末から通信ネットワークを介して公開情報にアクセスすると、その公開情報は、公開情報掲示機能により第三者に提供される。その際、閲覧アクセスログ記録サーバにおいて、第三者によって閲覧された公開情報とその公開情報に対するアクセス日時とが閲覧アクセスログとして獲得され保存される。

【 0 0 0 9 】

このようにして、第三者により閲覧された公開情報について、その内容と閲覧日時とが閲覧アクセスログとして記録されることになる。従って、この閲覧アクセスログにより、少なくともその閲覧日時には、その公開情報が電子データとして通信ネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを立証することができる。

【 0 0 1 0 】

本発明の掲載アクセスログ記録サーバ（請求項 3）は、通信ネットワークを介して情報提供サーバに送信・掲載された公開情報と該公開情報の掲載日時とを掲載アクセスログとして獲得する掲載アクセスログ獲得機能と、該掲載アクセスログ獲得機能によって獲得された該掲載アクセスログを保存する掲載アクセスログ保存機能とを有することを特徴としている。

【 0 0 1 1 】

上述の構成により、公開情報の掲載希望者が、その公開情報を、通信ネットワークを介して情報提供サーバに送信して掲載する際、掲載アクセスログ記録サーバにおいて、掲載希望者によって掲載された公開情報とその公開情報の掲載日時とが掲載アクセスログとして記録されることになる。従って、この掲載アクセスログにより、その掲載日時以降、その公開情報が電子データとして通信ネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを立証することができる。

【 0 0 1 2 】

さらに、本発明のデジタル署名サーバ（請求項 4）は、上述した情報提供サー

バおよび閲覧アクセスログ記録サーバとともに、公開立証システムを構成するものであって、該閲覧アクセスログにタイムスタンプを付加するタイムスタンプ付加機能と、該タイムスタンプを付加された該閲覧アクセスログを、該デジタル署名サーバの秘密鍵を用いて暗号化することにより、該タイムスタンプ付き閲覧アクセスログにデジタル署名を施す暗号化機能とを有することを特徴としている。

【0013】

上述の構成により、閲覧アクセスログ記録サーバで得られた閲覧アクセスログにタイムスタンプを付加した状態で、デジタル署名サーバの秘密鍵を用いてデジタル署名が施される。このデジタル署名サーバを第三者である電子公証会社等のものとするこゝで、閲覧アクセスログの証拠能力を高めることができる。

【0014】

そして、本発明の閲覧アクセス用情報端末（請求項5）は、上述した情報提供サーバおよび閲覧アクセスログ記録サーバとともに、公開立証システムを構成するものであって、該閲覧アクセスログ記録サーバにおいて該公開情報に対する閲覧アクセスログを意図的に残すことを目的として、該情報提供サーバにおける該公開情報に対する閲覧アクセスを定期的に行なうことを特徴としている。

【0015】

このような閲覧アクセス用情報端末により、閲覧アクセスログ記録サーバにおいて公開情報に対する閲覧アクセスログが定期的に且つ自動的に記録・保存される。従って、この閲覧アクセスログにより、少なくとも、この閲覧アクセス用情報端末が定期的な閲覧アクセスを行なっていた期間については、その公開情報が電子データとして通信ネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを立証することができる。

【0016】

【発明の実施の形態】

以下、図面を参照して本発明の実施の形態を説明する。

〔1〕第1実施形態の説明

図1は本発明の第1実施形態としての公開立証システムの構成を示すブロック

図であり、この図 1 に示すように、第 1 実施形態の公開立証システム 1 A は、情報提供サーバ 1 0 と公開情報アクセスログ記録サーバ（閲覧アクセスログ記録サーバ） 2 0 A とをそなえて構成されている。

【 0 0 1 7 】

情報提供サーバ 1 0 は、通信ネットワーク 2 を介して、情報端末 3 0 に対し公開情報の提供を行なうもので、後述するデータ送受信機能 1 1，公開情報保存機能 1 2 および公開情報掲示機能 1 3 を有している。なお、本実施形態では、通信ネットワーク 2 が、インターネット上に構築された WWW（World Wide Web）である場合について説明する。

【 0 0 1 8 】

また、公開情報アクセスログ記録サーバ 2 0 A は、通信ネットワーク 2 上において情報提供サーバ 1 0 と情報端末 3 0 との間に配置され、情報端末 3 0 による情報提供サーバ 1 0（公開情報）に対するアクセスログを記録すべく、後述するデータ送受信機能 2 1，データトラップ機能 2 2 およびデータ保存機能 2 3 を有している。本実施形態において、情報提供サーバ 1 0 と情報端末 3 0 との間で送受信されるデータ群は、公開情報アクセスログ記録サーバ 2 0 A を経由・通過するようになっている。

【 0 0 1 9 】

情報提供サーバ 1 0 において、データ送受信機能 1 1 は、通信ネットワーク 2 を介し、公開情報アクセスログ記録サーバ 2 0 A へ情報を送信したり公開情報アクセスログ記録サーバ 2 0 A から情報を受信したりするためのものである。

また、公開情報保存機能 1 2 は、提供すべき公開情報を電子データとして保存するためのものである。

【 0 0 2 0 】

さらに、公開情報掲示機能 1 3 は、公開情報を閲覧すべく通信ネットワーク 2 を介してアクセスしてきた情報端末 3 0 に対しその公開情報を提供するために、その公開情報（電子データ）を、公開情報保存機能 1 2 から読み出して、データ送受信機能 1 1，通信ネットワーク 2 および公開情報アクセスログ記録サーバ 2 0 A を通じて情報端末 3 0 に返送するものである。

【 0 0 2 1 】

一方、公開情報アクセスログ記録サーバ（閲覧アクセスログ記録サーバ）20Aにおいて、データ送受信機能21は、通信ネットワーク2を介し、情報提供サーバ10や情報端末30へ情報を送信したり情報提供サーバ10や情報端末30から情報を受信したりするためのものである。

また、データトラップ機能（閲覧アクセスログ獲得機能）22は、情報端末30により通信ネットワーク2を介して閲覧された公開情報と、その公開情報に対するアクセス日時を含む、情報端末30のアクセスログとを閲覧アクセスログ（公開情報アクセスログ、閲覧アクセス記録証拠データ群）として獲得するものである。

【 0 0 2 2 】

つまり、データトラップ機能22は、情報端末30から情報提供サーバ10に対する閲覧アクセスが行なわれた場合、情報端末30と情報提供サーバ10との間で通信ネットワーク2を介してやり取りされるデータ群（公開情報アクセスログ記録サーバ20Aを経由・通過するデータ群）から、上述した各種データを閲覧アクセスログとしてトラップするものである。

【 0 0 2 3 】

なお、ここでは、データトラップ機能22が、閲覧された公開情報と情報端末30のアクセスログとの両方を獲得するものとしているが、このデータトラップ機能22を、公開情報とアクセスログとをそれぞれ獲得する別々の機能（例えば閲覧データトラップ機能とアクセスログ機能と）に分離してもよい。

【 0 0 2 4 】

図2は、本実施形態において獲得・保存されるアクセスログの例を説明するための図であり、この図2に示すように、アクセスログとしては、アクセス年月日およびアクセス時刻のほかに、ドメイン情報、リモートホスト情報、ブラウザ名称情報や参照ディレクトリ情報などが含まれる。また、アクセスログは上述したものに限られず、公開情報にアクセスした情報端末（アクセス元）30にかかる端末情報、例えば、閲覧者（情報端末30）側の通信ネットワークアドレス、氏名、アクセス経路などをアクセスログとしてさらに獲得してもよい。

【 0 0 2 5 】

さらに、データ保存機能（閲覧アクセスログ保存機能）23は、データトラップ機能22によってトラップされた、公開情報データとアクセスログとをペアにし、閲覧アクセスログ（公開情報アクセスログ、閲覧アクセス記録証拠データ群）として保存するためのものである。

なお、情報端末30は、上述したように情報提供サーバ10における公開情報を検索・閲覧するために用いられるもので、例えばパーソナルコンピュータや携帯電話等の情報端末機器であり、データ送受信機能31およびWWWブラウザ32を有している。

【 0 0 2 6 】

ここで、データ送受信機能31は、通信ネットワーク2を介し、公開情報アクセスログ記録サーバ20Aへ情報を送信したり公開情報アクセスログ記録サーバ20Aから情報を受信したりするためのものである。WWWブラウザ（インターネットブラウザソフトウェア）32は、通信ネットワーク2を介して即ちWWWにより、情報提供サーバ10に対する閲覧アクセス等を行なう際に用いられるものである。

【 0 0 2 7 】

また、情報提供サーバ10は例えばパーソナルコンピュータ等の計算機により構成されており、上述したデータ送受信機能11、公開情報保存機能12および公開情報掲示機能13は、計算機上に搭載されるハードウェアやソフトウェアによって実現される。

同様に、公開情報アクセスログ記録サーバ20Aも例えばパーソナルコンピュータ等の計算機により構成されており、上述したデータ送受信機能21、データトラップ機能22およびデータ保存機能23は、計算機上に搭載されるハードウェアやソフトウェアによって実現される。

【 0 0 2 8 】

次に、上述のごとく構成された第1実施形態の公開立証システム1Aおよび公開情報アクセスログ記録サーバ20Aの動作について、図3に示すフローチャート（ステップS11～S16）に従って説明する。

情報提供サーバ10における公開情報の閲覧を希望する者（閲覧者、第三者）は、情報端末30（WWWブラウザ32）を起動して通信ネットワーク2に接続し、情報提供サーバ10に対する閲覧アクセスを、通信ネットワーク2を介して行なう（ステップS11）。

【0029】

そして、情報端末30は、まず、公開情報アクセスログ記録サーバ20Aにアクセスしてから（ステップS12）、情報提供サーバ10にアクセスし（ステップS13）、情報提供サーバ10における公開情報を閲覧することが可能な状態となる。

情報提供サーバ10では、公開情報揭示機能13により、情報端末30からの指示に応じて、閲覧者の望む公開情報が、公開情報保存機能12から検索されて読み出され、公開情報アクセスログ記録サーバ20Aを経由して情報端末30に返送され、閲覧者に提供される（ステップS14）。

【0030】

公開情報が公開情報アクセスログ記録サーバ20Aを経由する際、公開情報アクセスログ記録サーバ20Aにおいては、データトラップ機能22により、閲覧者（第三者）が閲覧した公開情報と、その公開情報に対するアクセス日時を含む情報端末30のアクセスログとが、閲覧アクセスログとしてトラップされ（ステップS15）、データ保存機能23によって保存される（ステップS16）。

【0031】

上述のごとく、公開立証システム1Aは、閲覧者側の情報端末30から情報提供サーバ10上の公開情報をアクセスする場合、公開情報アクセスログ記録サーバ20Aを経由してアクセスする仕組みとなっている。そして、公開情報アクセスログ記録サーバ20Aでは、情報端末30からアクセス・閲覧された公開情報の内容データとアクセス日時等を含むアクセスログとが、閲覧アクセスログとして保存される。アクセスログとしては、アクセス日時のみに限らず、閲覧者側の通信ネットワークアドレス、氏名、アクセス経路等の端末情報をトラップして保存する。このようにして閲覧された公開情報データとアクセスログとをペアにして保存することで、前記公開情報データが公開情報としてアクセス可能であった

という証拠を残すことが可能になる。

【 0 0 3 2 】

このように、本発明の第 1 実施形態としての公開立証システム 1 A や公開情報アクセスログ記録サーバ 2 0 A によれば、第三者である閲覧者により閲覧された公開情報について、その内容と閲覧日時とが閲覧アクセスログとして記録され、公開情報の公開履歴を、閲覧アクセスログにより証明可能な形式で保存することができるので、少なくともその閲覧日時には、その公開情報が電子データとして通信ネットワーク 2 上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク 2 上で掲示・公開されていたことを立証することができる。従って、情報提供サーバ 1 0 により通信ネットワーク 2 上で公開された情報に、印刷物や出版物と同様の証拠能力をもたせることができる。

【 0 0 3 3 】

また、第 1 実施形態の公開立証システム 1 A や公開情報アクセスログ記録サーバ 2 0 A を用いることにより、電子公証だけでなく、情報開示の開示記録や、アクセスが可能であったことの証明を行なうサービスを提供することができ、新規ビジネス創出の可能性が大きく広がる。

【 0 0 3 4 】

さらに、閲覧アクセスログとして、公開情報にアクセスした情報端末 3 0 にかかる端末情報（通信ネットワークアドレス、氏名、アクセス経路など）を獲得し保存することにより、閲覧アクセスログに含まれる端末情報に基づいて、どの情報端末 3 0 がどのような経路で公開情報に対して閲覧アクセスを行なったかを特定することが可能になり、閲覧アクセスログの証拠能力をより高めることができる。

【 0 0 3 5 】

またさらに、本実施形態の公開立証システム 1 A を用いて、電子データが通信ネットワーク 2 上で第三者が閲覧可能な状態で公開されていた日時を立証するサービスを提供することにより、様々な局面で電子データを証拠として使用することが可能になる。

例えば、P L (Product Liability) 法の立場から言えば、企業側が、製品の

問題情報や回収情報を Web（通信ネットワーク 2）上に公開し閲覧可能な状況にしていた期間を証明することが可能になり、企業側が通知義務に対して努力をしていたことを証明できる。

【 0 0 3 6 】

逆に、消費者側は、本サービスを利用することで、企業が、ある特定ページを公開していたという事実を第三者デジタル署名を行なって記録保存することにより、誇大広告や契約違反の証拠を残すことも可能になる。つまり、情報提供サーバ 1 0 の管理者側が本サービスを使用するのではなく、情報アクセス側が本サービスを利用するのである。また、Web（通信ネットワーク 2）上での公開掲示板に誹謗中傷の文書が記載された場合にも本公開立証システム 1 A を使用することにより名誉毀損の証拠を確実に残すことが可能になる。

【 0 0 3 7 】

なお、上述した第 1 実施形態では、便宜上、情報提供サーバ 1 0 と公開情報アクセスログ記録サーバ 2 0 A とを分けて説明したが、情報提供サーバ 1 0 としての機能と公開情報アクセスログ記録サーバ 2 0 A としての機能との両方を、物理的に一つのサーバマシンの中に組み込むことも可能である。ここで言うサーバとは、機能としてのサーバである。このように一つのサーバを、情報提供サーバ 1 0 および公開情報アクセスログ記録サーバ 2 0 A として兼用することにより、2 種類のサーバを別々にそなえる必要がなくなり、公開立証システム 1 A をより簡素に構成することができる。

【 0 0 3 8 】

また、公開情報アクセスログ記録サーバ 2 0 A としての機能をインターネットサービスプロバイダのプロキシサーバ内に組み込んでもよい。この場合、情報端末 3 0 において一般に用いられる WWW ブラウザ（インターネットブラウザソフトウェア）3 2 によって指定されるプロキシサーバを、公開情報アクセスログ記録サーバ 2 0 A としての機能を有するプロキシサーバに変更するだけで、情報端末 3 0 は、公開立証システム 1 A を容易に利用することができるほか、インターネットサービスプロバイダが新しいサービスを容易に提供することも可能になる。

【 0 0 3 9 】

さらに、公開情報アクセスログ記録サーバ20Aのデータ保存機能23が、閲覧アクセスログに含まれる公開情報データを圧縮した形で保存してもよい。ハードディスク等の記憶容量を考えると、アクセスログと一緒に保存される、閲覧された公開情報データについては、そのまま保存するよりも、圧縮して保存する方が望ましい。このような圧縮を行なうことにより、閲覧アクセスログを実際に保存するためのハードディスク等の記憶領域を効率的に利用することができる。

【0040】

〔2〕第2実施形態の説明

図4は本発明の第2実施形態としての公開立証システムの構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているため、その詳細な説明は省略する。

【0041】

図4に示すように、第2実施形態の公開立証システム1Bも、第1実施形態の公開立証システム1Aとほぼ同様に構成されているが、第2実施形態の公開立証システム1Bでは、第1実施形態の公開情報アクセスログ記録サーバ20Aに代えて公開情報アクセスログ記録サーバ（閲覧アクセスログ記録サーバ）20Bがそなえられている。この公開情報アクセスログ記録サーバ20Bは、第1実施形態と同様のデータ送受信機能21、データトラップ機能22およびデータ保存機能23のほかに、メッセージダイジェスト生成機能24をさらに有している。

【0042】

メッセージダイジェスト生成機能24は、データトラップ機能22によりトラップされた公開情報のメッセージダイジェストを生成するものであり、この第2実施形態のデータ保存機能23においては、公開情報そのものに代えて、メッセージダイジェスト生成機能24により公開情報（閲覧情報）の内容データから生成されたメッセージダイジェストが閲覧アクセスログとして保存されるようになっている。

【0043】

なお、メッセージダイジェストを作成するには、例えばMD5（Message Digest algorithm 5）等のアルゴリズムが使用される。また、メッセージダイジェス

ト生成機能 2 4 により、閲覧アクセスログの全てについてのメッセージダイジェストを生成してデータ保存機能 2 3 に保存するように構成してもよい。即ち、情報端末 3 0 のアクセスログについてのメッセージダイジェストも生成し、第 2 実施形態のデータ保存機能 2 3 において、情報端末 3 0 のアクセスログそのものに代え、メッセージダイジェスト生成機能 2 4 によりアクセスログから生成されたメッセージダイジェストを保存してもよい。

【 0 0 4 4 】

また、公開情報アクセスログ記録サーバ 2 0 B も、第 1 実施形態の公開情報アクセスログ記録サーバ 2 0 A と同様、例えばパーソナルコンピュータ等の計算機により構成されており、データ送受信機能 2 1、データトラップ機能 2 2、データ保存機能 2 3 およびメッセージダイジェスト生成機能 2 4 は、計算機上に搭載されるハードウェアやソフトウェアによって実現される。

【 0 0 4 5 】

次に、上述のごとく構成された第 2 実施形態の公開立証システム 1 B および公開情報アクセスログ記録サーバ 2 0 B の動作について、図 5 に示すフローチャート（ステップ S 2 1 ～ S 2 7）に従って説明する。

情報提供サーバ 1 0 における公開情報の閲覧を希望する者（閲覧者、第三者）は、第 1 実施形態と同様、情報端末 3 0（WWWブラウザ 3 2）を起動して通信ネットワーク 2 に接続し、情報提供サーバ 1 0 に対する閲覧アクセスを、通信ネットワーク 2 を介して行なう（ステップ S 2 1）。

【 0 0 4 6 】

そして、情報端末 3 0 は、まず、公開情報アクセスログ記録サーバ 2 0 B にアクセスしてから（ステップ S 2 2）、情報提供サーバ 1 0 にアクセスし（ステップ S 2 3）、情報提供サーバ 1 0 における公開情報を閲覧することが可能な状態となる。

情報提供サーバ 1 0 では、公開情報揭示機能 1 3 により、情報端末 3 0 からの指示に応じて、閲覧者の望む公開情報が、公開情報保存機能 1 2 から検索されて読み出され、公開情報アクセスログ記録サーバ 2 0 B を経由して情報端末 3 0 に返送され、閲覧者に提供される（ステップ S 2 4）。

【0047】

公開情報が公開情報アクセスログ記録サーバ20Bを経由する際、公開情報アクセスログ記録サーバ20Bにおいては、データトラップ機能22により、閲覧者（第三者）が閲覧した公開情報と、その公開情報に対するアクセス日時を含む情報端末30のアクセスログとが、閲覧アクセスログとしてトラップされる（ステップS25）。

【0048】

そして、第2実施形態においては、データトラップ機能22によりトラップされた公開情報データのメッセージダイジェストが、メッセージダイジェスト生成機能24により作成され（ステップS26）、このメッセージダイジェストと情報端末30のアクセスログとがペアでデータ保存機能23により保存される（ステップS27）。

【0049】

上述のごとく、公開立証システム1Bは、第1実施形態の公開立証システム1Aと同様、閲覧者側の情報端末30から情報提供サーバ10上の公開情報をアクセスする場合、公開情報アクセスログ記録サーバ20Bを経由してアクセスする仕組みとなっている。そして、公開情報アクセスログ記録サーバ20Bでは、情報端末30からアクセス・閲覧された公開情報の内容データから作成したメッセージダイジェストと、アクセス日時等を含むアクセスログとが、閲覧アクセスログとして保存される。

【0050】

この場合、情報提供サーバ10により公開・掲示された公開情報についてはその公開・掲示を終了した後も、公開情報保存機能12により保存しておく必要がある。なぜならば、公開情報のメッセージダイジェストを公開の証拠として用いる際には、公開情報保存機能12により保存しておいた公開情報から、メッセージダイジェスト生成機能24で使用されたものと同じアルゴリズムによりメッセージダイジェストを生成し、生成されたメッセージダイジェストと閲覧アクセスログに含まれているメッセージダイジェストとをつき合わせ、全く同じメッセージダイジェストが生成されるか否かを確認する必要があるからである。

【0051】

また、情報端末30のアクセスログを、公開情報アクセスログ記録サーバ20B側ではなく情報提供サーバ10側で保存し、公開情報アクセスログ記録サーバ20B側では、閲覧アクセスログのうちのメッセージダイジェストだけを保存してもよい。

例えば公開情報アクセスログ記録サーバ20Bが複数の情報提供サーバ10における公開情報の閲覧記録を管理するような場合、記憶媒体の容量を考えると、公開情報をそのまま保存するよりも、公開情報の内容データをメッセージダイジェストの形で保存しておく方が現実的である。

【0052】

また、データ量の少ない、情報端末30のアクセスログについてはそのままの状態公開情報アクセスログ記録サーバ20Bに保存することで、情報端末30のアクセスログについて、情報提供サーバ10における記録フォーマットと公開情報アクセスログ記録サーバ20Bにおける記録フォーマットとを一致させる必要がなくなる。

【0053】

従って、閲覧アクセスログのうち、公開情報データの内容のみをメッセージダイジェスト化して保存し、情報端末30のアクセスログはそのまま保存するという組み合わせが实际的である。

以上のようにして、閲覧された公開情報データのメッセージダイジェストとアクセスログとをペアにし、閲覧アクセスログ（閲覧アクセス記録証拠データ群）として保存することにより、前記公開情報データが公開情報としてアクセスが可能であったという証拠を残すことが可能になる。

【0054】

このように、本発明の第2実施形態としての公開立証システム1Bや公開情報アクセスログ記録サーバ20Bによれば、第1実施形態と同様の作用効果が得られるほか、公開情報データをメッセージダイジェストの形で保存することで、閲覧アクセスログを実際に保存するためのハードディスク等の記憶領域を効率的に利用することができる。

【 0 0 5 5 】

〔 3 〕 第 3 実施形態の説明

図 6 は本発明の第 3 実施形態としての公開立証システムの構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているため、その詳細な説明は省略する。

【 0 0 5 6 】

図 6 に示すように、第 3 実施形態の公開立証システム 1 C も、第 2 実施形態の公開立証システム 1 B とほぼ同様に構成されているが、第 3 実施形態の公開立証システム 1 C では、第 2 実施形態の公開情報アクセスログ記録サーバ 2 0 B に代えて公開情報アクセスログ記録サーバ（閲覧アクセスログ記録サーバ） 2 0 C がそなえられている。この公開情報アクセスログ記録サーバ 2 0 C は、第 2 実施形態と同様のデータ送受信機能 2 1，データトラップ機能 2 2，データ保存機能 2 3 およびメッセージダイジェスト生成機能 2 4 のほかに、暗号化機能 2 5 をさらに有している。

【 0 0 5 7 】

暗号化機能 2 5 は、公開情報アクセスログ記録サーバ 2 0 C のデータ保存機能 2 3 によって保存されるべき閲覧アクセスログを、公開情報アクセスログ記録サーバ 2 0 C の秘密鍵を用いて暗号化することにより、その閲覧アクセスログにデジタル署名を施すためのものである。

【 0 0 5 8 】

つまり、暗号化機能 2 5 は、公開情報アクセスログ記録サーバ 2 0 C のデータ保存機能 2 3 により閲覧アクセスログとして保存される、閲覧された公開情報データもしくはそのメッセージダイジェストと、その公開情報に対する閲覧アクセスを行なった情報端末 3 0 のアクセスログもしくはそのメッセージダイジェストとに対して、公開情報アクセスログ記録サーバ 2 0 C の秘密鍵を使用してデジタル署名を行なうものである。ただし、第 3 実施形態における暗号化機能 2 5 は、公開情報データのメッセージダイジェストと情報端末 3 0 のアクセスログとを含む閲覧アクセスログに対して、公開情報アクセスログ記録サーバ 2 0 C の秘密鍵を使用してデジタル署名を行なうものとする。

【0059】

なお、公開情報アクセスログ記録サーバ20Cも、第1実施形態の公開情報アクセスログ記録サーバ20Aと同様、例えばパーソナルコンピュータ等の計算機により構成されており、データ送受信機能21、データトラップ機能22、データ保存機能23、メッセージダイジェスト生成機能24および暗号化機能25は、計算機上に搭載されるハードウェアやソフトウェアによって実現される。

【0060】

次に、上述のごとく構成された第3実施形態の公開立証システム1Cおよび公開情報アクセスログ記録サーバ20Cの動作について、図7に示すフローチャート（ステップS31～S38）に従って説明する。

情報提供サーバ10における公開情報の閲覧を希望する者（閲覧者、第三者）は、第2実施形態と同様、情報端末30（WWWブラウザ32）を起動して通信ネットワーク2に接続し、情報提供サーバ10に対する閲覧アクセスを、通信ネットワーク2を介して行なう（ステップS31）。

【0061】

そして、情報端末30は、まず、公開情報アクセスログ記録サーバ20Cにアクセスしてから（ステップS32）、情報提供サーバ10にアクセスし（ステップS33）、情報提供サーバ10における公開情報を閲覧することが可能な状態となる。

情報提供サーバ10では、公開情報揭示機能13により、情報端末30からの指示に応じて、閲覧者の望む公開情報が、公開情報保存機能12から検索されて読み出され、公開情報アクセスログ記録サーバ20Cを経由して情報端末30に返送され、閲覧者に提供される（ステップS34）。

【0062】

公開情報が公開情報アクセスログ記録サーバ20Cを経由する際、公開情報アクセスログ記録サーバ20Cにおいては、データトラップ機能22により、閲覧者（第三者）が閲覧した公開情報と、その公開情報に対するアクセス日時を含む情報端末30のアクセスログとが、閲覧アクセスログとしてトラップされ（ステップS35）、トラップされた公開情報データのメッセージダイジェストが、メ

ッセージダイジェスト生成機能 2 4 により作成される（ステップ S 3 6）。

【0 0 6 3】

そして、第 3 実施形態においては、暗号化機能 2 5 により、公開情報データのメッセージダイジェストと情報端末 3 0 のアクセスログとからなる閲覧アクセスログが、公開情報アクセスログ記録サーバ 2 0 C の秘密鍵により暗号化されてデジタル署名を施されてから（ステップ S 3 7）、デジタル署名を施された閲覧アクセスログがデータ保存機能 2 3 により保存される（ステップ S 3 8）。

【0 0 6 4】

上述のごとく、公開立証システム 1 C は、第 2 実施形態の公開立証システム 1 B と同様、閲覧者側の情報端末 3 0 から情報提供サーバ 1 0 上の公開情報をアクセスする場合、公開情報アクセスログ記録サーバ 2 0 C を経由してアクセスする仕組みとなっている。そして、公開情報アクセスログ記録サーバ 2 0 C では、デジタル署名を施された閲覧アクセスログが保存される。

【0 0 6 5】

このように、本発明の第 3 実施形態としての公開立証システム 1 C や公開情報アクセスログ記録サーバ 2 0 C によれば、第 1 および第 2 実施形態と同様の作用効果が得られるほか、閲覧アクセスログがデジタル署名を施されて保存されるので、閲覧アクセスログが改ざんされるのを確実に防止することができ、閲覧アクセスログの証拠能力をより高めることができる。

【0 0 6 6】

〔4〕第 4 実施形態の説明

図 8 は本発明の第 4 実施形態としての公開立証システムの構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているため、その詳細な説明は省略する。

【0 0 6 7】

図 8 に示すように、第 4 実施形態の公開立証システム 1 D も、第 3 実施形態の公開立証システム 1 C とほぼ同様に構成されているが、第 4 実施形態の公開立証システム 1 D においては、第 3 実施形態と同様の情報提供サーバ 1 0 および公開情報アクセスログ記録サーバ 2 0 C のほかに、第三者デジタル署名サーバ 4 0 が

さらにそなえられている。

【 0 0 6 8 】

この第三者デジタル署名サーバ40は、例えば電子公証会社に属するものであって、通信ネットワーク2を介して公開情報アクセスログ記録サーバ20Cと通信可能に接続され、公開情報アクセスログ記録サーバ20Cにおいてデジタル署名を施された閲覧アクセスログ（閲覧アクセス記録証拠データ群）に対しさらなるデジタル署名を施すべく、後述するデータ送受信機能41，タイムスタンプ付加機能42および暗号化機能43を有している。

【 0 0 6 9 】

ここで、データ送受信機能41は、通信ネットワーク2を介して、公開情報アクセスログ記録サーバ20Cへ情報（例えばデジタル署名を施した閲覧アクセスログ等）を送信したり公開情報アクセスログ記録サーバ20Cから情報（例えばデジタル署名を施すべき閲覧アクセスログ等）を受信したりするためのものである。

【 0 0 7 0 】

また、タイムスタンプ付加機能42は、データ送受信機能41により受信した情報（ここでは公開情報アクセスログ記録サーバ20Cにおいてデジタル署名を施された閲覧アクセスログ）を受信すると、その閲覧アクセスログにタイムスタンプ（例えば、その閲覧アクセスログを受信した年月日および時刻）を付加するものである。

【 0 0 7 1 】

さらに、暗号化機能43は、タイムスタンプを付加された閲覧アクセスログを、第三者デジタル署名サーバ40の秘密鍵を用いて暗号化することにより、そのタイムスタンプ付き閲覧アクセスログにデジタル署名を施すものである。

そして、このようにデジタル署名を施されたタイムスタンプ付き閲覧アクセスログが、データ送受信機能41により通信ネットワーク2を介して公開情報アクセスログ記録サーバ20Cに返送され、データ保存機能23によって保存されるようになっている。

【 0 0 7 2 】

なお、第三者デジタル署名サーバ40に、暗号化機能43によってデジタル署名を施された、タイムスタンプ付き閲覧アクセスログを保存するデータ保存機能（閲覧アクセスログ保存機能）44をさらにそなえてもよい。この場合、デジタル署名を施された、タイムスタンプ付き閲覧アクセスログを、上述のごとく公開情報アクセスログ記録サーバ20Cに返送してデータ保存機能23にも保存させてもよいし、第三者デジタル署名サーバ40のデータ保存機能44にのみ保存してもよい。

【0073】

次に、上述のごとく構成された第4実施形態の公開立証システム1Dおよび第三者デジタル署名サーバ40の動作について、図9に示すフローチャート（ステップS31～S37およびS41～S46）に従って説明する。なお、図9に示すステップS31～S37の処理は図7に示したものと同様であるので、その説明は省略する。

【0074】

第4実施形態においては、公開情報アクセスログ記録サーバ20Cの暗号化機能25によりデジタル署名を施された閲覧アクセスログ（閲覧アクセス記録証拠データ群）は、データ送受信機能21により通信ネットワーク2を介して第三者デジタル署名サーバ40に送信される（ステップS41）。

【0075】

そして、第三者デジタル署名サーバ40のデータ送受信機能41により、公開情報アクセスログ記録サーバ20Cからの閲覧アクセスログが受信されると（ステップS42）、受信したデータに対し、タイムスタンプ付加機能42によりタイムスタンプが付加された後、タイムスタンプ付きの閲覧アクセスログが、暗号化機能43により、第三者デジタル署名サーバ40の秘密鍵により暗号化されてデジタル署名を施される（ステップS43）。

【0076】

この後、ステップS43でデジタル署名（暗号化）を施された閲覧アクセスログは、データ送受信機能41により通信ネットワーク2を介して公開情報アクセスログ記録サーバ20Cに送信される（ステップS44）。

そして、公開情報アクセスログ記録サーバ 2 0 C のデータ送受信機能 2 1 により、第三者デジタル署名サーバ 4 0 からの、暗号化済み閲覧アクセスログが受信されると（ステップ S 4 5）、その暗号化済み閲覧アクセスログがデータ保存機能 2 3 により保存される（ステップ S 4 6）。

【0 0 7 7】

このように、本発明の第 4 実施形態としての公開立証システム 1 D や第三者デジタル署名サーバ 4 0 によれば、第 1 ～第 3 実施形態と同様の作用効果が得られるほか、公開情報アクセスログ記録サーバ 2 0 C で得られた閲覧アクセスログにタイムスタンプを付加した状態で、第三者デジタル署名サーバ 4 0 の秘密鍵を用いて、さらなるデジタル署名を施すことにより、この閲覧アクセスログが改ざんされるのをより確実に防止できるとともに、閲覧時刻にほぼ対応した日時（受信日時）がタイムスタンプとして付加されるので、閲覧アクセスログの証拠能力、つまりは証拠としての信頼性をより高めることができる。

【0 0 7 8】

なお、上述した第 4 実施形態では、閲覧アクセスログ（閲覧アクセス記録証拠データ群）に対して、公開情報アクセスログ記録サーバ 2 0 C と第三者デジタル署名サーバ 4 0 との両方においてデジタル署名を施す場合について説明したが、公開情報アクセスログ記録サーバ 2 0 C でのデジタル署名を省略し、第三者デジタル署名サーバ 4 0 でのデジタル署名のみを実行するように構成してもよい。

【0 0 7 9】

〔5〕第 5 実施形態の説明

図 1 0 は本発明の第 5 実施形態としての公開立証システムの構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているため、その詳細な説明は省略する。

【0 0 8 0】

図 1 0 に示すように、第 5 実施形態の公開立証システム 1 E も、第 4 実施形態の公開立証システム 1 D とほぼ同様に構成されているが、第 5 実施形態の公開立証システム 1 E においては、第 4 実施形態と同様の情報提供サーバ 1 0、公開情報アクセスログ記録サーバ 2 0 C や第三者デジタル署名サーバ 4 0 のほかに、複

数（図 1 0 中では 3 個）の閲覧アクセス用情報端末 5 0 がさらにそなえられている。

【 0 0 8 1 】

各閲覧アクセス用情報端末 5 0 は、公開情報アクセスログ記録サーバ 2 0 C において公開情報に対する閲覧アクセスログ（閲覧アクセス記録証拠データ群）を意図的に残すことを目的として、情報提供サーバ 1 0 における公開情報に対する閲覧アクセスを定期的（所定の時間毎）に行なうもので、例えばパーソナルコンピュータ等の情報端末機器であり、後述するデータ送受信機能 5 1，WWWブラウザ 5 2，アクセス期日指定機能 5 3 およびアクセスサイト指定データベース 5 4 を有している。また、これらの情報端末 5 0 は、例えば異なる複数の国にそれぞれ配置されているものとする。

【 0 0 8 2 】

ここで、データ送受信機能 5 1 は、通信ネットワーク 2 を介し、公開情報アクセスログ記録サーバ 2 0 A へ情報を送信したり公開情報アクセスログ記録サーバ 2 0 A から情報を受信したりするためのものである。

WWWブラウザ（インターネットブラウザソフトウェア）5 2 は、通信ネットワーク 2 を介して即ちWWWにより、情報提供サーバ 1 0 に対する閲覧アクセス等を行なう際に用いられるものである。

【 0 0 8 3 】

アクセス期日指定機能 5 3 は、情報端末 5 0 が情報提供サーバ 1 0 における公開情報に対してアクセス期日（期間，時間間隔）を指定するためのものであり、アクセスサイト指定データベース 5 4 は、情報端末 5 0 が閲覧アクセスを行なうべく指定されたアクセスサイト（即ち情報提供サーバ 1 0）のアドレスを予め保持するものである。

【 0 0 8 4 】

そして、情報端末 5 0 のWWWブラウザ 5 2 が、アクセス期日指定機能 5 3 によって指定されたアクセス期日に応じた所定の期間内の間、所定の時間毎に、アクセスサイト指定データベース 5 4 に予め登録された情報提供サーバ 1 0 の公開情報に対して、自動的に閲覧アクセスを行なうように構成されている。

【 0 0 8 5 】

次に、上述のごとく構成された第 5 実施形態の公開立証システム 1 E および閲覧アクセス用情報端末 5 0 の動作について、図 1 1 に示すフローチャート（ステップ S 5 1 ～ S 5 9）に従って説明する。

閲覧アクセス用情報端末 5 0 が起動されて通信ネットワーク 2 に接続されると（ステップ S 5 1）、情報端末 5 0（WWW ブラウザ 5 2）は、アクセス期日指定機能 5 3 によって指定されたアクセス期日を参照するとともに（ステップ S 5 2）、データベース 5 4 を参照して、予め指定された情報提供サーバ 1 0 のアドレスを読み出し（ステップ S 5 3）、アクセス期日に応じた所定の期間内の間、所定の時間毎に、指定された情報提供サーバ 1 0 の公開情報に対する閲覧アクセスを自動的に行なう（ステップ S 5 4 ～ S 5 6）。

【 0 0 8 6 】

このとき、情報端末 5 0 は、前述した情報端末 3 0 の場合と同様、まず、公開情報アクセスログ記録サーバ 2 0 C を経由して（ステップ S 5 4）、情報提供サーバ 1 0 にアクセスし（ステップ S 5 5）、情報提供サーバ 1 0 における公開情報を閲覧することが可能な状態となる。

そして、情報提供サーバ 1 0 では、情報端末 5 0 からの指示に応じて、公開情報揭示機能 1 3 により、公開情報が公開情報保存機能 1 2 から検索されて読み出され、公開情報アクセスログ記録サーバ 2 0 C を経由して情報端末 5 0 に返送される（ステップ S 5 6）。

【 0 0 8 7 】

これに伴って、公開情報アクセスログ記録サーバ 2 0 C および第三者デジタル署名サーバ 4 0 により、図 9 に示すステップ S 3 5 ～ S 3 7 および S 4 1 ～ S 4 6 の処理が実行され、公開情報アクセスログ記録サーバ 2 0 C に閲覧アクセスログ（閲覧アクセス記録証拠データ群）が保存される（ステップ S 5 7）。

この後、閲覧アクセス用情報端末 5 0 は、閲覧アクセスについてのアクセスログを保存すると（ステップ S 5 8）、通信ネットワーク 2 から切断され停止される（ステップ S 5 9）、一連の閲覧アクセス処理を終了する。

【 0 0 8 8 】

上述のごとく、公開立証システム 1 E では、情報提供サーバ 1 0 や公開情報アクセスログ記録サーバ 2 0 C が、閲覧者側の情報端末 3 0（図 1 等参照）からの閲覧アクセスが発生するのを待つのではなく、公開立証システム 1 E の運用者側が、インターネット経由で情報提供サーバ 1 0 における公開情報に対し、所定期間に亘って定期的にアクセスする情報端末 5 0 を予め設置し、この情報端末 5 0 により、公開情報に対する閲覧アクセスを積極的に発生させている。

【 0 0 8 9 】

これにより、閲覧アクセスログ（閲覧アクセス記録証拠データ群）が公開情報アクセスログ記録サーバ 2 0 C に積極的に残されることになり、アクセス期日として予め指定した期間に亘り、情報提供サーバ 1 0 における公開情報が閲覧可能であったという証拠を確実に残すことが可能になる。

また、情報端末 5 0 を海外に設置することで、他国からのアクセスも可能であったことを証明することができる。さらには、パリ条約加盟国全てに情報端末 5 0 を設置して情報アクセスが可能であったことを記録することで、情報提供サーバ 1 0 で開示していた情報を特許公知例情報として主張することも可能になる。

【 0 0 9 0 】

このように、本発明の第 5 実施形態としての公開立証システム 1 E や閲覧アクセス用情報端末 5 0 によれば、第 1 ～ 第 4 実施形態と同様の作用効果が得られるほか、閲覧アクセス用情報端末 5 0 が公開情報に対する閲覧アクセスを定期的に行なうことにより、公開情報アクセスログ記録サーバ 2 0 C において公開情報に対する閲覧アクセスログが定期的に且つ自動的に記録・保存される。

【 0 0 9 1 】

従って、第三者（例えば、前述した情報端末 3 0）から公開情報に対する閲覧アクセスがなくても、閲覧アクセス用情報端末 5 0 による閲覧アクセス期間を予め決めておけば、少なくともその期間について、その公開情報が電子データとして通信ネットワーク 2 上において誰でもまた海外からもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク 2 上で掲示・公開されていたことを確実に立証することができる。

【 0 0 9 2 】

これにより、通信ネットワーク 2 上で掲示・公開された情報に、より確実に、印刷物や出版物と同様の証拠能力をもたせることができる。

また、電子文書が作成された日付のみならず、その電子文書が公開情報として通信ネットワーク 2 経由で外部からアクセス可能であった時期と期間とを証明することが可能になる。

【 0 0 9 3 】

〔 5 - 1 〕 第 5 実施形態の第 1 変形例の説明

図 1 2 は本発明の第 5 実施形態としての公開立証システムの第 1 変形例の構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

図 1 2 に示すように、第 1 変形例の公開立証システム 1 E - 1 も、第 5 実施形態の公開立証システム 1 E とほぼ同様に構成されているが、第 1 変形例の公開立証システム 1 E - 1 においては、通信ネットワーク 2 と複数の閲覧アクセス用情報端末 5 0 との間に、それぞれ、インターネットサービスプロバイダのサーバ 3 が介在している。つまり、各閲覧アクセス用情報端末 5 0 が、インターネットサービスプロバイダのサーバ 3 を経由して通信ネットワーク 2 に接続されている。

【 0 0 9 4 】

次に、上述のごとく構成された第 5 実施形態の第 1 変形例の公開立証システム 1 E - 1 の動作について、図 1 3 に示すフローチャート（ステップ S 5 1 ～ S 6 0）に従って説明する。なお、図 1 3 に示すステップ S 5 1 ～ S 5 9 の処理は図 1 1 に示したものとほぼ同様であるので、その詳細な説明は省略する。

【 0 0 9 5 】

第 5 実施形態の第 1 変形例においては、各閲覧アクセス用情報端末 5 0 が、公開情報アクセスログ記録サーバ 2 0 C を経由して情報提供サーバ 1 0 の公開情報にアクセスする際に、インターネットサービスプロバイダのサーバ 3 を経由して通信ネットワーク 2 に接続されるため、前述したステップ S 5 3 とステップ S 5 4 との間で、新たなステップ S 6 0 の処理が実行されている。

【 0 0 9 6 】

つまり、図 1 3 に示すように、ステップ S 5 3 の処理後、情報端末 5 0 は、イ

ンターネットサービスプロバイダのサーバ 3 にダイヤルアップ接続され（ステップ S 6 0）、そのサーバ 3 を通し、さらに通信ネットワーク 2 および公開情報アクセスログ記録サーバ 2 0 C を経由して情報提供サーバ 1 0 にアクセスする（ステップ S 5 4, S 5 5）。

【 0 0 9 7 】

なお、図 1 1 に示したステップ S 5 1 では、情報端末 5 0 が起動されて通信ネットワーク 2 に接続されているが、この第 1 変形例では、上述のごとく、ステップ S 5 9 において情報端末 5 0 が通信ネットワーク 2 に接続されるようになっていたため、図 1 3 に示すステップ S 5 1 では、情報端末 5 0 が起動されるだけである。

【 0 0 9 8 】

このようにして、所定の Web サイト（情報提供サーバ 1 0）に対して複数かつ多国籍のプロバイダから所定の公開情報アクセスログ記録サーバ 2 0 C を経由して各企業の Web サイトにアクセスする仕組みを構築することができる。

そして、公開情報アクセスログ記録サーバ 2 0 C に保存される閲覧アクセスログ（情報端末 5 0 のアクセスログ）内に、プロバイダのサーバ 3 経由で閲覧アクセスが行なわれた旨の記録が残ることになるため、より信頼性の高いアクセス情報を残すことができる。つまり、特定の IP（Internet Protocol）アドレスや通信ネットワークドメインからのアクセスではなく、メジャーなプロバイダのサーバ 3 を経由するダイヤルアップ接続で公開情報にアクセスする可能であったことを証明することができる。

【 0 0 9 9 】

〔 5 - 2 〕 第 5 実施形態の第 2 変形例の説明

図 1 4 は本発明の第 5 実施形態としての公開立証システムの第 2 変形例の構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているため、その詳細な説明は省略する。

図 1 4 に示すように、第 2 変形例の公開立証システム 1 E - 2 も、第 5 実施形態の公開立証システム 1 E とほぼ同様に構成されているが、第 2 変形例の公開立証システム 1 E - 2 においては、インターネットサービスプロバイダのプロキシ

サーバ 4 が公開情報アクセスログ記録サーバ 2 0 C としての機能を有している。

【 0 1 0 0 】

このような公開立証システム 1 E - 2 によれば、インターネットサービスプロバイダのプロキシサーバ 4 に、閲覧アクセスログ記録サーバ 2 0 C としての機能を組み込むことにより、情報端末 5 0 において一般に用いられる WWW ブラウザ（インターネットブラウザソフトウェア） 5 2 により指定されるプロキシサーバを、閲覧アクセスログ記録サーバ 2 0 C としての機能を有するプロキシサーバ 4 に変更するだけで、情報端末 5 0 は公開立証システム 1 E - 2 を容易に利用することができるほか、インターネットサービスプロバイダが新しいサービスを容易に提供することも可能になる。

【 0 1 0 1 】

さらには、各国に専用の情報端末 5 0 を設置し、その情報端末 5 0 から、所定の日時や時刻に、上述したプロキシサーバ 4 を経由して Web サイト（情報提供サーバ 1 0）に自動的にアクセスすることにより、プロキシサーバ 4 や第三者デジタル署名サーバ 4 0 において、情報提供サーバ 1 0 の公開情報が各国から閲覧可能であったという証拠を自動的に且つ確実に残すことが可能になる。

【 0 1 0 2 】

〔 6 〕 第 6 実施形態の説明

第 6 実施形態では、後で詳述するごとく、例えば、情報提供サーバ 1 0 として発明技術公開サーバ 6 0（図 1 5 参照）を設定する。

この発明技術公開サーバ 6 0 では、サーバ運用者と利用契約を結んでいる契約者の発明技術情報を常に情報公開するようにする。契約者は特許権利化がグレーの領域にある発明を行なった場合に特許出願を行なう代わりに、匿名にて発明技術公開サーバ 6 0 に公開情報として発明技術情報を掲載する。

【 0 1 0 3 】

この情報を掲載する際には、運用者側は例えば契約者 ID とパスワードとでアクセス管理を行なう。このとき、運用者側は、例えば 1 件当たりの情報掲載料を課金・徴収する。

契約者側は、発明技術公開サーバ 6 0 に技術を公開することで、自身の発明の

特許化は断念することになるが、他社が同様な特許を出願して権利化することを抑止することができる。また、従来の技術公開情報のように紙ベースではなく、電子ベースでの開示になるため、発案して即開示することも可能で、従来のように開示準備中に他者に特許出願されてしまう可能性も低く抑えることができる。

【0104】

つまり、近年のように細分化された特許が出願される状況では、会社によってはその出願費用が嵩む場合が出てくる。その反面、特許出願をしなくて、且つ、アイデアのままで保持している場合には、他社が出願した場合にその技術を使用することができなくなってしまう。

そこで、公開期間が証明され、且つ、誰でもアクセス可能な形で発明技術公開サーバ60を運用することで、発明者にとっての最悪状況を回避させることができる。なお、匿名で情報を開示するのは、誰がどのような発明を行なっているかという技術開発動向を調査されることを回避するためである。

【0105】

さらには、契約者が発明技術公開サーバ60に発明技術情報を掲載したときのアクセスログとデータ内容とを、第1～第5実施形態で説明したものと同様の手法で掲載アクセスログとして保存することにより、その発明技術情報がいつから掲載されているかの証拠も残すことが可能になる。また、その発明情報を何処の誰が掲載したかという情報についても、契約者IDにより特定することが可能になる。

【0106】

図15は本発明の第6実施形態としての公開立証システムの構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているので、その詳細な説明は省略する。

第6実施形態では、情報が公開情報であったことを立証する本発明の仕組み（公開立証システム）を、より具体的な例、即ち、上述したような、発明技術情報を一般に公開するためのシステムに適用した場合について説明する。

【0107】

従って、第6実施形態の公開立証システム1Fは、図15に示すように、第5

実施形態の公開立証システム 1 E とほぼ同様に構成されているが、第 6 実施形態の公開立証システム 1 F においては、第 5 実施形態の情報提供サーバ 1 0 に代えて発明技術公開サーバ 6 0 がそなえられるとともに、第 5 実施形態の公開情報アクセスログ記録サーバ 2 0 C に代えて公開情報アクセスログ記録サーバ 7 0 がそなえられている。

【 0 1 0 8 】

なお、第 6 実施形態では、公開情報（ここでは発明技術情報）の掲載希望者がその情報を発明技術公開サーバ 6 0 に送信・掲載するための掲載アクセス用情報端末 8 0 がそなえられている。この掲載アクセス用情報端末 8 0 は、例えばパーソナルコンピュータ等の情報端末機器であり、前述した情報端末 3 0 や 5 0 と同様のデータ送受信機能 8 1 および WWW ブラウザ（インターネットブラウザソフトウェア） 8 2 を有するほか、前記発明技術情報を予め保存するための掲示用発明技術情報保存機能 8 3 を有している。

【 0 1 0 9 】

また、掲載希望者には、発明技術公開サーバ 6 0 の運用者と予め利用契約を結ぶことにより、予め識別情報（利用者 ID、契約者 ID）とパスワード（パスフレーズ）とが付与されており、掲載希望者は、発明技術情報を情報端末 8 0 から発明技術公開サーバ 6 0 に送信して掲載する際には、それに先立ち、その識別情報およびパスワードを、情報端末 8 0 から通信ネットワーク 2 を経由して発明技術公開サーバ 6 0 に送信するようになっている。

【 0 1 1 0 】

そして、発明技術公開サーバ（情報提供サーバ） 6 0 は、データ送受信機能 6 1、発明技術情報保存機能 6 2、発明技術情報掲示機能 6 3、発明技術情報登録機能 6 4 および課金情報更新機能 6 5 を有している。

データ送受信機能 6 1、発明技術情報保存機能 6 2 および発明技術情報掲示機能 6 3 は、それぞれ、前述したデータ送受信機能 2 1、公開情報保存機能 2 2 および公開情報掲示機能 2 3 に対応している。ただし、発明技術情報保存機能 6 2 および発明技術情報掲示機能 6 3 が、公開情報として、より具体的な発明技術情報を取り扱っている点だけが異なっている。

【0111】

また、発明技術情報登録機能64は、情報端末80から送信されてきた識別情報とパスワードとに基づいて掲載希望者の確認を行なった後、情報端末80から送信されてきた発明技術情報を発明技術情報保存機能62に登録して保存・掲載するためのものである。

さらに、課金情報更新機能65は、発明技術情報登録機能64により発明技術情報の登録を行なった場合、その情報の掲載者（契約者）から情報掲載料を徴収すべく、識別情報に対応した、掲載者についての課金情報更新するためのものである。

【0112】

なお、上述した発明技術公開サーバ60も例えばパーソナルコンピュータ等の計算機により構成されており、上述したデータ送受信機能61，発明技術情報保存機能62，発明技術情報掲示機能63，発明技術情報登録機能64および課金情報更新機能65は、計算機上に搭載されるハードウェアやソフトウェアによって実現される。

【0113】

一方、公開情報アクセスログ記録サーバ70は、上述した機能21～25にそれぞれ対応する、データ送受信機能71，データトラップ機能72，データ保存機能73，メッセージダイジェスト生成機能74および暗号化機能75を有している。

【0114】

ただし、第6実施形態における公開情報アクセスログ記録サーバ70は、前述した公開情報アクセスログ記録サーバ20Cと同様の機能つまり閲覧アクセスログ記録サーバとしての機能のほかに、情報端末80からの発明技術情報の掲載アクセスに際し、発明技術情報のデータ内容とその掲載日時とを含む掲載アクセスログを獲得して保存する、掲載アクセスログ記録サーバとしての機能を併せもつものである。

【0115】

このため、データトラップ機能（閲覧アクセスログ獲得機能，掲載アクセスロ

グ保存機能) 72は、前述したデータトラップ機能22と同様の機能を果たすほかに、情報端末80から通信ネットワーク2を介して発明技術公開サーバ60に送信・掲載される発明技術情報と、その掲載日時を含む、情報端末80のアクセスログとを掲載アクセスログ(公開情報アクセスログ, 掲載アクセス記録証拠データ群)として獲得する掲載アクセスログ獲得機能としての機能を果たすものである。

【0116】

つまり、データトラップ機能72は、情報端末30(図15では図示省略)や情報端末50から発明技術公開サーバ60に対する閲覧アクセスが行なわれた場合、あるいは、情報端末80から発明技術公開サーバ60に対する掲載アクセスが行なわれた場合、これらの情報端末30, 50, 80と発明技術公開サーバ60との間で通信ネットワーク2を介してやり取りされるデータ群(公開情報アクセスログ記録サーバ70を経由・通過するデータ群)から、上述した各種データを閲覧アクセスログあるいは掲載アクセスログとしてトラップするものである。

【0117】

なお、掲載アクセスログに含まれる、情報端末80のアクセスログとしては、図2を参照しながら前述したもののほかに、発明技術情報を送信した情報端末80にかかる端末情報、例えば、閲覧者(情報端末80)側の通信ネットワークアドレス、氏名、アクセス経路や、前述した識別情報(契約者ID)などをさらに獲得してもよい。

【0118】

また、データ保存機能(閲覧アクセスログ保存機能, 掲載アクセスログ保存機能)73は、前述したデータ保存機能23と同様、データトラップ機能72によってトラップされた閲覧アクセスログもしくは掲載アクセスログを保存するためのものである。このデータ保存機能73において、閲覧アクセスログもしくは掲載アクセスログは、データトラップ72で獲得された形式のまま保存されてもよいが、本実施形態では、後述するメッセージダイジェスト生成機能74, 暗号化機能75および第三者デジタル署名サーバ40によって処理を施された形式で保存されるようになっている。

【0119】

メッセージダイジェスト生成機能74は、例えばMD5 (Message Digest algorithm 5) 等のアルゴリズムを使用して、データトラップ機能22によりトラップされた発明技術情報のメッセージダイジェストを生成するものである。このとき、メッセージダイジェスト生成機能74により、閲覧アクセスログや掲載アクセスログの全てについてのメッセージダイジェストを生成してもよい。

【0120】

このとき、データ保存機能73においては、発明技術情報のメッセージダイジェストと、情報端末30, 50, 80のアクセスログとをペアにして、閲覧アクセスログもしくは掲載アクセスログとして保存してもよいし、閲覧アクセスログや掲載アクセスログの全てについて生成されたメッセージダイジェストを保存してもよい。

【0121】

暗号化機能75は、データ保存機能73によって保存されるべき閲覧アクセスログもしくは掲載アクセスログを、公開情報アクセスログ記録サーバ70の秘密鍵を用いて暗号化することにより、その閲覧アクセスログもしくは掲載アクセスログにデジタル署名を施すためのものである。

【0122】

このとき、データ保存機能73においては、暗号化機能75により、データトラップ機能72で獲得された形式のままの、閲覧アクセスログもしくは掲載アクセスログを暗号化した結果を保存してもよいし、メッセージダイジェスト生成機能74により生成されたメッセージダイジェストを含む閲覧アクセスログもしくは掲載アクセスログを暗号化した結果を保存してもよい。さらに、データ保存機能73においては、第4実施形態で前述したように、第三者デジタル署名サーバ40を用いて暗号化を施された閲覧アクセスログもしくは掲載アクセスログを保存してもよい。

【0123】

なお、上述した公開情報アクセスログ記録サーバ70も例えばパーソナルコンピュータ等の計算機により構成されており、上述したデータ送受信機能71、デ

ータトラップ機能 7 2, データ保存機能 7 3, メッセージダイジェスト生成機能 7 4 および暗号化機能 7 5 は、計算機上に搭載されるハードウェアやソフトウェアによって実現される。

また、本実施形態では、公開情報アクセスログ記録サーバ 7 0 が、閲覧アクセスログ記録サーバとしての機能と掲載アクセスログ記録サーバとしての機能とを併せもっているが、これらの機能をそれぞれ異なるサーバにそなえてもよい。

【 0 1 2 4 】

次に、上述のごとく構成された第 6 実施形態の公開立証システム 1 F, 発明技術公開サーバ 6 0 および公開情報アクセスログ記録サーバ 7 0 の動作について、図 1 6 に示すフローチャート（ステップ S 6 1 ～ S 7 0）に従って説明する。

なお、発明技術公開サーバ 6 0 によって掲示・公開される発明技術情報に対する閲覧アクセス、および、その閲覧アクセスに伴う閲覧アクセスログ（閲覧アクセス記録証拠データ群）の記録・保存は、前述した実施形態と同様に行なわれるので、その説明は省略する。

【 0 1 2 5 】

従って、ここでは、発明技術情報の掲載希望者（既に発明技術公開サーバ 6 0 の運用者と利用契約を結んでいる契約者）が、その発明技術情報を発明技術公開サーバ 6 0 に掲載する処理（掲載アクセス）について、図 1 6 を参照しながら詳細に説明する。

【 0 1 2 6 】

まず、掲載希望者は、掲載アクセス用情報端末 8 0 を起動して（ステップ S 6 1）、通信ネットワーク 2 に接続し（ステップ S 6 2）、公開情報アクセスログ記録サーバ 7 0 を経由して発明技術公開サーバ 6 0 にアクセスし（ステップ S 6 3）、この発明技術公開サーバ 6 0 における発明技術掲載メニューにアクセスする（ステップ S 6 4）。

【 0 1 2 7 】

そして、掲載希望者は、発明技術掲載メニューの指示に従って、予め付与されている契約者 ID およびパスワードを入力し（ステップ S 6 5）、発明技術公開サーバ 6 0 側において、入力された契約者 ID およびパスワードに基づいて掲載

希望者が契約者である旨が確認されると、発明情報掲載メニューにログインする（ステップ S 6 6）。

【 0 1 2 8 】

ついで、掲載希望者は、発明技術公開サーバ 6 0 での掲示・公開を希望する発明技術情報（発明データ）を、情報端末 8 0 から公開情報アクセスログ記録サーバ 7 0 を経由して発明技術公開サーバ 6 0 に送信する（ステップ S 6 7）。

このとき、公開情報アクセスログ記録サーバ 7 0 および第三者デジタル署名サーバ 4 0 により、例えば図 9 に示すステップ S 3 5 ～ S 3 7 および S 4 1 ～ S 4 6 と同様の処理が実行され、公開情報アクセスログ記録サーバ 7 0 （もしくは第三者デジタル署名サーバ 4 0 ）に、発明技術情報の内容と、少なくとも掲載日時を含む情報端末 8 0 のアクセスログとが、掲載アクセスログ（掲載アクセス記録証拠データ群）として保存される（ステップ S 6 8）。

【 0 1 2 9 】

この後、掲載アクセス用情報端末 8 0 は、今回の掲載アクセスについてのアクセスログを保存すると（ステップ S 6 9）、掲載希望者が、情報端末 8 0 を通信ネットワーク 2 から切断して停止し（ステップ S 7 0）、一連の掲載アクセス処理を終了する。

【 0 1 3 0 】

このように、本発明の第 6 実施形態としての公開立証システム 1 F、発明技術公開サーバ 6 0 および公開情報アクセスログ記録サーバ 7 0 によれば、第 1 ～ 第 5 実施形態と同様の作用効果が得られるほかに、以下のような作用効果が得られる。

（a）発明技術公開サーバ 6 0 に送信・掲載された発明技術情報について、その内容と掲載日時とが掲載アクセスログとして公開情報アクセスログ記録サーバ 7 0 もしくは第三者デジタル署名サーバ 4 0 に記録・保存されるので、公開情報の掲載履歴を、掲載アクセスログにより証明可能な形式で保存することができるので、その掲載日時以降、その公開情報が電子データとして通信ネットワーク（インターネット）2 上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク 2 上で掲示・公開されていたことを立証する

ことができる。従って、通信ネットワーク 2 上で公開された情報に、印刷物や出版物と同様の証拠能力をもたせることができる。

【0 1 3 1】

(b) 上述のごとく電子データに印刷物や出版物と同様の証拠能力をもたせることが可能になったことで、通信ネットワーク（インターネット）2 上で公開された電子データを例えば特許の公知例として採用することが可能になる。

このとき、技術開発側から考えた場合、確実に情報公開を行なえ且つその情報公開期間を立証できるサービスが上述のごとく提供されることで、他社が権利化することを恐れて瑣末なアイデア等を全て特許や実用新案として出願することがなくなり、企業の特許出願費用の削減と特許庁に対する負荷の軽減とを実現可能になる。

【0 1 3 2】

(c) 匿名の形で新規技術の公開サービスを行なうことが可能になり、クライアントの企業は開発動向を知られることなく、新規技術を公知情報として公開することが可能になる。従って、各企業や個人は、特許になるかならないか分からない技術を公知情報として開示記録を残すことができ、そのような技術を無理やり特許として出願するのを抑止でき、特許出願にかかる費用を削減することが可能になる。

【0 1 3 3】

(d) 従来の技術公開情報のように紙ベースではなく、電子ベースで発明技術情報が開示されるため、発案して即開示することも可能で、従来の印刷物の技術公開公報と比較してリリースまでの時間を大幅に短縮することができ、公開準備をしている間に他者に同様のアイデアを出願される危険性が減る。

(e) 上述のような公開立証システム 1 F を用いることにより、発明技術公開サーバ 6 0 側は、契約者 ID とパスワードとを用いて発明技術情報の掲載アクセス管理を行なうことができ、例えば公開情報 1 件ごとに情報掲載料を課金・徴収するといった、新たな情報掲載サービスを容易に提供することが可能になる。

【0 1 3 4】

(f) 公開情報アクセスログ記録サーバ 7 0 が、閲覧アクセスログ記録サーバ

が掲載アクセスログ記録サーバとしての機能を兼ねることにより、異なる２種類のサーバをそなえる必要がなくなり、公開立証システム１Ｆをより簡素に構成することができる。

【０１３５】

〔６－１〕第６実施形態の変形例の説明

第６実施形態の変形例は、発明技術情報を発明技術公開サーバ６０において掲示する際に情報掲載者についての匿名性をより高めたい場合に対応したものであり、契約者がプリペイドカードを購入し、そのプリペイドカードに記された識別情報（ＩＤ）とパスワードとを用いて発明技術公開サーバ６０の発明情報情報掲示機能６３にアクセスするための手法が示されている。このとき、発明技術公開サーバ６０では、同一ＩＤによるアクセス回数（情報掲載回数）をカウントし、そのカウント値が所定の回数に到達した時点で、発明技術情報掲載機能６３へのログインを止めるように構成してもよい。この場合は、契約者が発明技術情報を事前に第三者デジタル署名サーバもしくは電子公証サーバに送り、タイムスタンプを加えてデジタル署名を受けておくことが望ましい。

【０１３６】

図１７は本発明の第６実施形態としての公開立証システムの変形例の構成を示すブロック図であり、図中、既述の符号と同一の符号は同一もしくはほぼ同一の部分を示しているため、その詳細な説明は省略する。

図１７に示すように、第６実施形態の変形例の公開立証システム１Ｆ－１も、第６実施形態の公開立証システム１Ｆとほぼ同様に構成されているが、この公開立証システム１Ｆ－１では、第６実施形態の発明技術公開サーバ６０に代えて発明技術公開サーバ（情報提供サーバ）６０－１がそなえられている。この発明技術公開サーバ６０－１は、第６実施形態と同様のデータ送受信機能６１，発明技術情報保存機能６２，発明技術情報掲示機能６３および発明技術情報登録機能６４を有するとともに、課金情報更新機能６５に代えてプリペイド残高更新機能６６を有している。

【０１３７】

なお、公開立証システム１Ｆ－１では、発明技術公開サーバ６０の運用者によ

って、識別情報（ID）とパスワードとを記載したプリペイドカードが予め発行され、発明技術情報の掲載希望者は、そのプリペイドカードを予め購入することになる。

【0138】

そして、この変形例における発明技術情報登録機能64は、情報端末80から送信されてきた識別情報（ID）とパスワードとが、既に発行され且つ未だ全度数を使用していないプリペイドカードに記載されたものであることを確認することにより、掲載希望者の確認を行なった後、情報端末80から送信されてきた発明技術情報を発明技術情報保存機能62に登録して保存・掲載するようになっている。

【0139】

また、プリペイド残高更新機能66は、プリペイドカードの残存度数（残り使用回数）を、発明技術情報の発明技術公開サーバ60への掲載回数に対応・連動させるためのものである。なお、このプリペイド残高更新機能66は、前述したごとく、同一IDによるアクセス回数（情報掲載回数）をカウントするものとしてもよい。この場合、発明技術情報登録機能64は、そのカウント値が所定の回数に到達した時点で、発明技術情報掲載機能63へのログインを止めるように動作することになる。

【0140】

次に、上述のごとく構成された第6実施形態の変形例の公開立証システム1F-1の動作について、図18に示すフローチャート（ステップS71～S83）に従って説明する。

公開立証システム1F-1では、前述した通り、発明技術公開サーバ60の運用者が、識別情報（ID）とパスワードとを記載したプリペイドカードを発行しており、発明技術情報の掲載希望者は、そのプリペイドカードを購入して（ステップS71）、IDとパスワードとを取得する（ステップS72）。

【0141】

そして、掲載希望者は、掲載アクセス用情報端末80を起動して（ステップS73）、通信ネットワーク2に接続し（ステップS74）、公開情報アクセスロ

グ記録サーバ70を経由して発明技術公開サーバ60にアクセスし（ステップS75）、この発明技術公開サーバ60における発明技術掲載メニューにアクセスする（ステップS76）。

【0142】

そして、掲載希望者は、発明技術掲載メニューの指示に従って、購入したプリペイドカードに記載されたIDおよびパスワードを入力し（ステップS77）、発明技術公開サーバ60側において、入力されたIDおよびパスワードが、既に発行され且つ未だ全度数を使用していないプリペイドカードに記載されたものであることが確認されると、発明情報掲載メニューにログインする（ステップS78）。

【0143】

ついで、掲載希望者は、発明技術公開サーバ60での掲示・公開を希望する発明技術情報（発明データ）を、情報端末80から公開情報アクセスログ記録サーバ70を経由して発明技術公開サーバ60に送信される（ステップS79）。これに応じて、発明技術公開サーバ60において、その発明技術情報が、発明技術情報登録機能64によって発明技術情報保存機能62に登録されると、プリペイド残高更新機能66により、当該IDを付与されたプリペイドカードについて、残存度数（残り使用回数）を減じるように度数の更新が行なわれる（ステップS80）。

【0144】

また、このとき、公開情報アクセスログ記録サーバ70および第三者デジタル署名サーバ40により、例えば図9に示すステップS35～S37およびS41～S46と同様の処理が実行され、公開情報アクセスログ記録サーバ70（もしくは第三者デジタル署名サーバ40）に、発明技術情報の内容と、少なくとも掲載日時を含む情報端末80のアクセスログとが、掲載アクセスログ（掲載アクセス記録証拠データ群）として保存される（ステップS81）。

【0145】

この後、掲載アクセス用情報端末80は、今回の掲載アクセスについてのアクセスログを保存すると（ステップS82）、掲載希望者が、情報端末80を通信

ネットワーク 2 から切断して停止し（ステップ S 8 3）、一連の掲載アクセス処理を終了する。

【 0 1 4 6 】

このようにな公開立証システム 1 F - 1 によれば、発明技術情報の掲載料を徴収した後に、掲載希望者の、より高い匿名性を確保しながら発明技術情報を発明技術公開サーバ 6 0 で公開することができる。従って、匿名での情報掲載サービスを提供することも可能になる。

【 0 1 4 7 】

〔 7 〕 その他

なお、本発明は上述した実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で種々変形して実施することができる。

例えば、上述した第 6 実施形態では、公開情報が発明技術情報である場合について説明したが、本発明は、これに限定されるものではない。

【 0 1 4 8 】

〔 8 〕 付記

（付記 1） 提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報掲示機能とを有する情報提供サーバと、

該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとをそなえたことを特徴とする、公開立証システム。

【 0 1 4 9 】

（付記 2） 該閲覧アクセスログ獲得機能が、該閲覧アクセスログとして、さらに、該公開情報にアクセスした該情報端末にかかる端末情報を獲得することを特徴とする、付記 1 記載の公開立証システム。

（付記 3） 該閲覧アクセスログ記録サーバが、さらに、該閲覧アクセスロ

グ獲得機能により獲得された該公開情報のメッセージダイジェストを生成するメッセージダイジェスト生成機能を有し、

該閲覧アクセスログ保存機能が、該メッセージダイジェストを該閲覧アクセスログにおける該公開情報として保存することを特徴とする、付記 1 または付記 2 に記載の公開立証システム。

【 0 1 5 0 】

(付記 4) 一つのサーバが、該情報提供サーバとしての機能と該閲覧アクセスログ記録サーバとしての機能との両方を果たすように構成されていることを特徴とする、付記 1 ～付記 3 のいずれか一つに記載の公開立証システム。

(付記 5) 該閲覧アクセスログ記録サーバが、さらに、該閲覧アクセスログ保存機能によって保存されるべき該閲覧アクセスログを、該閲覧アクセスログ記録サーバの秘密鍵を用いて暗号化することにより、該閲覧アクセスログにデジタル署名を施す暗号化機能を有していることを特徴とする、付記 1 ～付記 4 のいずれか一つに記載の公開立証システム。

【 0 1 5 1 】

(付記 6) 該閲覧アクセスログにタイムスタンプを付加するタイムスタンプ付加機能と、該タイムスタンプを付加された該閲覧アクセスログを、所定の秘密鍵を用いて暗号化することにより、該タイムスタンプ付き閲覧アクセスログにデジタル署名を施す暗号化機能とを有するデジタル署名サーバをさらにそなえ、

該閲覧アクセスログ記録サーバの該閲覧アクセスログ保存機能が、該デジタル署名サーバにおいてデジタル署名を施された、該タイムスタンプ付き閲覧アクセスログを保存することを特徴とする、付記 1 ～付記 5 のいずれか一つに記載の公開立証システム。

【 0 1 5 2 】

(付記 7) 該閲覧アクセスログにタイムスタンプを付加するタイムスタンプ付加機能と、該タイムスタンプを付加された該閲覧アクセスログを、所定の秘密鍵を用いて暗号化することにより、該タイムスタンプ付き閲覧アクセスログにデジタル署名を施す暗号化機能と、該暗号化機能によってデジタル署名を施された、該タイムスタンプ付き閲覧アクセスログを保存する閲覧アクセスログ保存機

能とを有するデジタル署名サーバをさらにそなえたことを特徴とする、付記 1 ～付記 5 のいずれか一つに記載の公開立証システム。

【 0 1 5 3 】

(付記 8) 該閲覧アクセスログ記録サーバにおいて該公開情報に対する閲覧アクセスログを意図的に残すことを目的として、該情報提供サーバにおける該公開情報に対する閲覧アクセスを定期的に行なう、少なくとも一つの閲覧アクセス用情報端末をさらにそなえたことを特徴とする、付記 1 ～付記 7 のいずれか一つに記載の公開立証システム。

【 0 1 5 4 】

(付記 9) 複数の該閲覧アクセス用情報端末が、複数の国にそれぞれ配置されていることを特徴とする、付記 8 記載の公開立証システム。

(付記 1 0) 該閲覧アクセス用情報端末が、インターネットサービスプロバイダのサーバを経由して該通信ネットワークに接続されていることを特徴とする、付記 8 または付記 9 に記載の公開立証システム。

【 0 1 5 5 】

(付記 1 1) インターネットサービスプロバイダのプロキシサーバが、該閲覧アクセスログ記録サーバとしての機能を有していることを特徴とする、付記 1 ～付記 1 0 のいずれか一つに記載の公開立証システム。

(付記 1 2) 該公開情報の掲載希望者が、該掲載希望者に対し予め付与された識別情報とパスワードとを、該通信ネットワークを介して該情報提供サーバに送信し、該情報提供サーバが、該識別情報と該パスワードとに基づき該掲載希望者の確認を行なった後に、該公開情報を保存・掲載することを特徴とする、付記 1 ～付記 1 1 のいずれか一つに記載の公開立証システム。

【 0 1 5 6 】

(付記 1 3) 該識別情報と該パスワードとが、該掲載希望者によって購入されたプリペイドカードに記載されたものであることを特徴とする、付記 1 2 記載の公開立証システム。

(付記 1 4) 該プリペイドカードの残存度数を、公開情報の該情報提供サーバへの掲載回数に対応させたことを特徴とする、付記 1 3 記載の公開立証シス

テム。

【0157】

(付記15) 該公開情報が該通信ネットワークを介して該情報提供サーバに掲載される際に該公開情報と該公開情報の掲載日時とを掲載アクセスログとして獲得する掲載アクセスログ獲得機能と、該掲載アクセスログ獲得機能によって獲得された該掲載アクセスログを保存する掲載アクセスログ保存機能とを有する掲載アクセスログ記録サーバをさらにそなえたことを特徴とする、付記1～付記14のいずれか一つに記載の公開立証システム。

【0158】

(付記16) 該閲覧アクセスログ記録サーバが該掲載アクセスログ記録サーバとしての機能を兼ね、該閲覧アクセスログ獲得機能が該掲載アクセスログ記録サーバとして機能するとともに、該閲覧アクセスログ保存機能が該掲載アクセスログ保存機能として機能するように構成されたことを特徴とする、付記15記載の公開立証システム。

【0159】

(付記17) 該閲覧アクセスログ記録サーバの閲覧アクセスログ保存機能が、該閲覧アクセスログに含まれる該公開情報を圧縮した形で保存していることを特徴とする、付記1～付記16のいずれか一つに記載の公開立証システム。

(付記18) 通信ネットワークを介して閲覧された公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有することを特徴とする、閲覧アクセスログ記録サーバ。

【0160】

(付記19) 該閲覧アクセスログ獲得機能が、該閲覧アクセスログとして、さらに、該公開情報にアクセスした該情報端末にかかる端末情報を獲得することを特徴とする、付記18記載の閲覧アクセスログ記録サーバ。

(付記20) 該閲覧アクセスログ獲得機能により獲得された該公開情報のメッセージダイジェストを生成するメッセージダイジェスト生成機能をさらに有

し、

該閲覧アクセスログ保存機能が、該メッセージダイジェストを該閲覧アクセスログにおける該公開情報として保存することを特徴とする、付記 1 8 または付記 1 9 に記載の閲覧アクセスログ記録サーバ。

【0 1 6 1】

(付記 2 1) 該閲覧アクセスログ保存機能によって保存されるべき該閲覧アクセスログを、該閲覧アクセスログ記録サーバの秘密鍵を用いて暗号化することにより、該閲覧アクセスログにデジタル署名を施す暗号化機能をさらに有していることを特徴とする、付記 1 8 ～付記 2 0 のいずれか一つに記載の閲覧アクセスログ記録サーバ。

【0 1 6 2】

(付記 2 2) 通信ネットワークを介して情報提供サーバに送信・掲載された公開情報と該公開情報の掲載日時とを掲載アクセスログとして獲得する掲載アクセスログ獲得機能と、該掲載アクセスログ獲得機能によって獲得された該掲載アクセスログを保存する掲載アクセスログ保存機能とを有することを特徴とする、掲載アクセスログ記録サーバ。

【0 1 6 3】

(付記 2 3) 提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報掲示機能とを有する情報提供サーバと、

該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとともに公開立証システムを構成するデジタル署名サーバであって、

該閲覧アクセスログにタイムスタンプを付加するタイムスタンプ付加機能と、該タイムスタンプを付加された該閲覧アクセスログを、該デジタル署名サーバの秘密鍵を用いて暗号化することにより、該タイムスタンプ付き閲覧アクセスログ

にデジタル署名を施す暗号化機能とを有することを特徴とする、デジタル署名サーバ。

【0164】

(付記24) 該暗号化機能によってデジタル署名を施された、該タイムスタンプ付き閲覧アクセスログを保存する閲覧アクセスログ保存機能をさらに有することを特徴とする、付記23記載のデジタル署名サーバ。

(付記25) 提供すべき公開情報を電子データとして保存する公開情報保存機能と、該公開情報を閲覧すべく通信ネットワークを介してアクセスしてきた情報端末に対し、該公開情報を提供する公開情報揭示機能とを有する情報提供サーバと、

該情報端末により該通信ネットワークを介して閲覧された該公開情報と該公開情報に対するアクセス日時とを閲覧アクセスログとして獲得する閲覧アクセスログ獲得機能と、該閲覧アクセスログ獲得機能によって獲得された該閲覧アクセスログを保存する閲覧アクセスログ保存機能とを有する閲覧アクセスログ記録サーバとともに公開立証システムを構成する情報端末であって、

該閲覧アクセスログ記録サーバにおいて該公開情報に対する閲覧アクセスログを意図的に残すことを目的として、該情報提供サーバにおける該公開情報に対する閲覧アクセスを定期的に行なうことを特徴とする、閲覧アクセス用情報端末。

【0165】

【発明の効果】

以上詳述したように、本発明の公開立証システム(請求項1)並びに閲覧アクセスログ記録サーバ(請求項2)、掲載アクセスログ記録サーバ(請求項3)およびデジタル署名サーバ(請求項4)並びに閲覧アクセス用情報端末(請求項5)によれば、以下のような効果ないし利点を得ることができる。

【0166】

(1) 第三者により閲覧された公開情報について、その内容と閲覧日時とが閲覧アクセスログとして記録されるので、公開情報の公開履歴を、閲覧アクセスログにより証明可能な形式で保存することができ、少なくともその閲覧日時には、その公開情報が電子データとして通信ネットワーク上において誰でもアクセス可

能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを立証することができる。従って、通信ネットワーク上で公開された情報に、印刷物や出版物と同様の証拠能力をもたせることができる（請求項1，2）。

【0167】

（2）情報提供サーバに送信・掲載された公開情報について、その内容と掲載日時とが掲載アクセスログとして記録されるので、公開情報の掲載履歴を、掲載アクセスログにより証明可能な形式で保存することができ、その掲載日時以降、その公開情報が電子データとして通信ネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを立証することができる。従って、通信ネットワーク上で公開された情報に、印刷物や出版物と同様の証拠能力をもたせることができる（請求項3）。

【0168】

（3）第三者である電子公証会社等のデジタル署名サーバにおいて、閲覧アクセスログ記録サーバで得られた閲覧アクセスログにタイムスタンプを付加した状態で、デジタル署名サーバの秘密鍵を用いてデジタル署名を施すことにより、この閲覧アクセスログが改ざんされるのを確実に防止できるほか、閲覧時刻にほぼ対応した日時がタイムスタンプとして付加されるので、閲覧アクセスログの証拠能力、つまりは証拠としての信頼性をより高めることができる（請求項4）。

【0169】

（4）閲覧アクセス用情報端末が公開情報に対する閲覧アクセスを定期的に行なうことにより、閲覧アクセスログ記録サーバにおいて公開情報に対する閲覧アクセスログが定期的に且つ自動的に記録・保存される。従って、第三者から公開情報に対する閲覧アクセスがなかった場合であっても、閲覧アクセス用情報端末による閲覧アクセス期間を予め決めておけば、少なくともその期間については、その公開情報が電子データとして通信ネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データが通信ネットワーク上で掲示・公開されていたことを確実に立証することができる。これにより、通信ネットワー

ク上で掲示・公開された情報に、より確実に、印刷物や出版物と同様の証拠能力をもたせることができる（請求項5）。

【0170】

（5）上述のごとく電子データに印刷物や出版物と同様の証拠能力をもたせることが可能になったことで、通信ネットワーク上で公開された電子データを例えば特許の公知例として採用することが可能になる。これにより、加熱し瑣末化する特許競争に伴って増加していた、企業の特許出願に係る費用を減らすことができるとともに、特許庁に無用の負担をかけることがなくなる。

【0171】

（6）上述のごとく電子データに印刷物や出版物と同様の証拠能力をもたせることが可能になったことで、ビジネス上、以下のような意義がある。

（6-1）電子公証だけでなく、情報開示の開示記録や、アクセスが可能であったことの証明を行なうサービスを提供することができ、新規ビジネス創出の可能性が大きく広がる。

【0172】

（6-2）匿名の形で新規技術の公開サービスを行なうことで、クライアントの企業は開発動向を知られることなく、新規技術を公知情報として公開することが可能になる。従って、特許になるかならないか分からない技術を無理やり特許として出願するのを抑止でき、特許出願にかかる費用を削減することが可能になる。

（6-3）従来の印刷物の技術公開公報と比較してリリースまでの時間（情報を公開するまでにかかる時間）を大幅に短縮することができるため、公開準備をしている間に他者に同様のアイデアを出願される危険性が減る。

【0173】

（7）電子データが通信ネットワーク上で第三者が閲覧可能な状態で公開されていた日時を立証するサービスを提供することで、様々な局面で電子データを証拠として使用することが可能になる。

（8）閲覧アクセスログとして、公開情報にアクセスした情報端末にかかる端末情報を獲得し保存することにより、閲覧アクセスログに含まれる端末情報に基

づいて、どの情報端末がどのような経路で公開情報に対して閲覧アクセスを行なったかを特定することが可能になり、閲覧アクセスログの証拠能力をより高めることができる。

【0174】

(9) 公開情報のメッセージダイジェストを生成し、このメッセージダイジェストを閲覧アクセスログにおける公開情報として保存することにより、閲覧アクセスログを実際に保存するためのハードディスク等の記憶領域を効率的に利用することができる。

(10) 一つのサーバを、情報提供サーバおよび閲覧アクセスログ記録サーバとして兼用することにより、2種類のサーバを別々にそなえる必要がなくなり、公開立証システムを簡素に構成することができる。

【0175】

(11) 閲覧アクセスログ記録サーバにおいて、閲覧アクセスログにデジタル署名を施して保存することにより、この閲覧アクセスログが改ざんされるのを確実に防止することができ、閲覧アクセスログの証拠能力を高めることが可能になる。

(12) 複数の閲覧アクセス用情報端末を複数の国にそれぞれ配置することにより、情報提供サーバにおける公開情報が複数の国から閲覧アクセス可能であったことを確実に証拠（閲覧アクセスログ）として残すことが可能になる。

【0176】

(13) 閲覧アクセス用情報端末がインターネットサービスプロバイダのサーバを経由して閲覧アクセスを行なうように構成することにより、閲覧アクセスログだけでなく、そのプロバイダのサーバにおいてアクセス記録が自動的に残るため、より信頼性の高いアクセス情報を残すことができる。

【0177】

(14) インターネットサービスプロバイダのプロキシサーバに、閲覧アクセスログ記録サーバとしての機能を組み込むことにより、情報端末において一般に用いられるインターネットブラウザソフトウェアにより指定されるプロキシサーバを、閲覧アクセスログ記録サーバとしての機能を有するプロキシサーバに変更す

るだけで、情報端末は本発明の公開立証システムを容易に利用することができるほか、インターネットサービスプロバイダが新しいサービスを容易に提供することも可能になる。

【 0 1 7 8 】

(1 5) 公開情報の掲載希望者が、その掲載希望者に対し予め付与された識別情報とパスワードとを、通信ネットワークを介して情報提供サーバに送信し、情報提供サーバが、識別情報とパスワードとに基づき掲載希望者の確認を行なった後に、公開情報を掲載するように構成することで、情報提供サーバ側は、その識別情報とパスワードとを用いて公開情報の掲載アクセス管理を行なうことができ、例えば公開情報 1 件ごとに情報掲載料を徴収するといった、新たな情報掲載サービスを容易に提供することが可能になる。

【 0 1 7 9 】

(1 6) 識別情報とパスワードとが掲載希望者によって購入されたプリペイドカードに記載されたものとし、また、プリペイドカードの残存度数を、公開情報の情報提供サーバへの掲載回数に対応させることで、公開情報の掲載料を徴収した後に、掲載希望者のより高い匿名性を確保しながら公開情報を情報提供サーバで公開することができる。従って、匿名での情報掲載サービスを提供することも可能になる。

【 0 1 8 0 】

(1 7) 閲覧アクセスログ記録サーバが掲載アクセスログ記録サーバとしての機能を兼ね、閲覧アクセスログ獲得機能が掲載アクセスログ記録サーバとして機能するとともに、閲覧アクセスログ保存機能が掲載アクセスログ保存機能として機能するように構成することにより、2種類のサーバを別々にそなえる必要がなくなり、公開立証システムを簡素に構成することができる。

【 0 1 8 1 】

(1 8) 閲覧アクセスログ記録サーバの閲覧アクセスログ保存機能が、閲覧アクセスログに含まれる公開情報を圧縮した形で保存することにより、閲覧アクセスログを実際に保存するためのハードディスク等の記憶領域を効率的に利用することができる。

【図面の簡単な説明】

【図 1】

本発明の第 1 実施形態としての公開立証システムの構成を示すブロック図である。

【図 2】

本実施形態において獲得・保存されるアクセスログの例を説明するための図である。

【図 3】

第 1 実施形態の動作を説明するためのフローチャートである。

【図 4】

本発明の第 2 実施形態としての公開立証システムの構成を示すブロック図である。

【図 5】

第 2 実施形態の動作を説明するためのフローチャートである。

【図 6】

本発明の第 3 実施形態としての公開立証システムの構成を示すブロック図である。

【図 7】

第 3 実施形態の動作を説明するためのフローチャートである。

【図 8】

本発明の第 4 実施形態としての公開立証システムの構成を示すブロック図である。

【図 9】

第 4 実施形態の動作を説明するためのフローチャートである。

【図 1 0】

本発明の第 5 実施形態としての公開立証システムの構成を示すブロック図である。

【図 1 1】

第 5 実施形態の動作を説明するためのフローチャートである。

【図 1 2】

本発明の第 5 実施形態としての公開立証システムの第 1 変形例の構成を示すブロック図である。

【図 1 3】

第 5 実施形態の第 1 変形例の動作を説明するためのフローチャートである。

【図 1 4】

本発明の第 5 実施形態としての公開立証システムの第 2 変形例の構成を示すブロック図である。

【図 1 5】

本発明の第 6 実施形態としての公開立証システムの構成を示すブロック図である。

【図 1 6】

第 6 実施形態の動作を説明するためのフローチャートである。

【図 1 7】

本発明の第 6 実施形態としての公開立証システムの変形例の構成を示すブロック図である。

【図 1 8】

第 6 実施形態の変形例の動作を説明するためのフローチャートである。

【符号の説明】

1 A, 1 B, 1 C, 1 D, 1 E, 1 E - 1, 1 E - 2, 1 F, 1 F - 1 公開立証システム

2 通信ネットワーク（インターネット）

3 インターネットサービスプロバイダのサーバ

4 インターネットサービスプロバイダのプロキシサーバ

1 0 情報提供サーバ

1 1 データ送受信機能

1 2 公開情報保存機能

1 3 公開情報揭示機能

2 0 A, 2 0 B, 2 0 C 公開情報アクセスログ記録サーバ（閲覧アクセスロ

グ記録サーバ)

- 2 1 データ送受信機能
- 2 2 データトラップ機能 (閲覧アクセスログ獲得機能)
- 2 3 データ保存機能 (閲覧アクセスログ保存機能)
- 2 4 メッセージダイジェスト生成機能
- 2 5 暗号化機能
- 3 0 情報端末
- 3 1 データ送受信機能
- 3 2 WWWブラウザ (インターネットブラウザソフトウェア)
- 4 0 第三者デジタル署名サーバ
- 4 1 データ送受信機能
- 4 2 タイムスタンプ付加機能
- 4 3 暗号化機能
- 4 4 データ保存機能 (閲覧アクセスログ保存機能)
- 5 0 閲覧アクセス用情報端末
- 5 1 データ送受信機能
- 5 2 WWWブラウザ (インターネットブラウザソフトウェア)
- 5 3 アクセス期日指定機能
- 5 4 アクセスサイト指定データベース
- 6 0, 6 0 - 1 発明技術公開サーバ (情報提供サーバ)
- 6 1 データ送受信機能
- 6 2 発明技術情報保存機能 (公開情報保存機能)
- 6 3 発明技術情報揭示機能 (公開情報揭示機能)
- 6 4 発明技術情報登録機能
- 6 5 課金情報更新機能
- 6 6 プリペイド残高更新機能
- 7 0 公開情報アクセスログ記録サーバ (閲覧アクセスログ記録サーバ, 掲載
アクセスログ記録サーバ)
- 7 1 データ送受信機能

7 2 データトラップ機能（閲覧アクセスログ獲得機能，掲載アクセスログ保存機能）

7 3 データ保存機能（閲覧アクセスログ保存機能，掲載アクセスログ保存機能）

7 4 メッセージダイジェスト生成機能

7 5 暗号化機能

8 0 掲載アクセス用情報端末

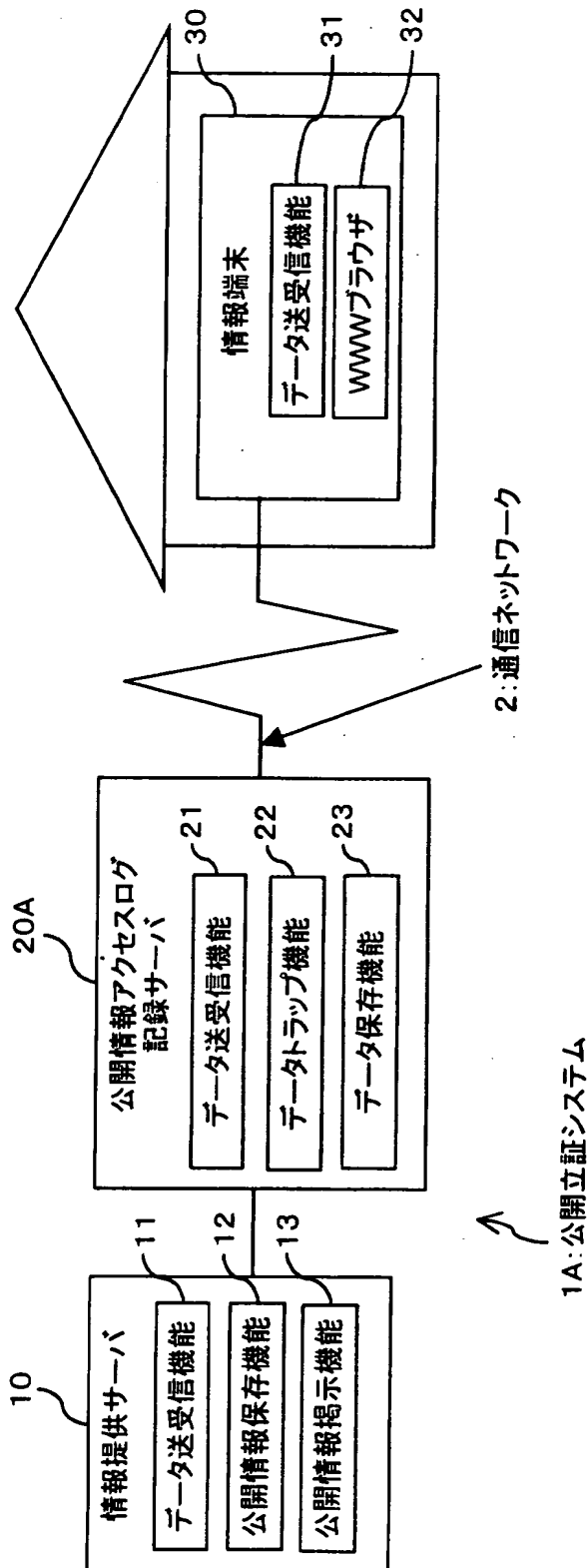
8 1 データ送受信機能

8 2 WWWブラウザ（インターネットブラウザソフトウェア）

8 3 掲示用発明技術情報保存機能

【書類名】 図面

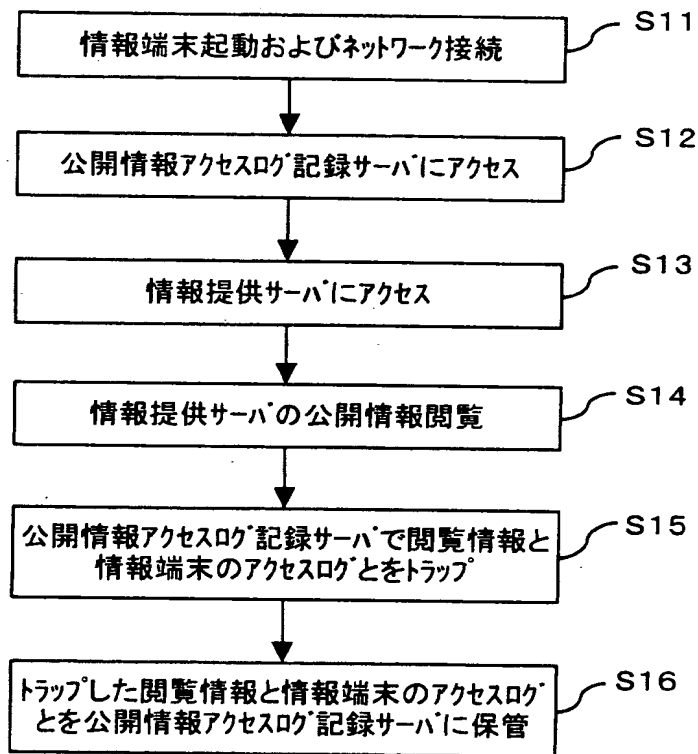
【図 1】



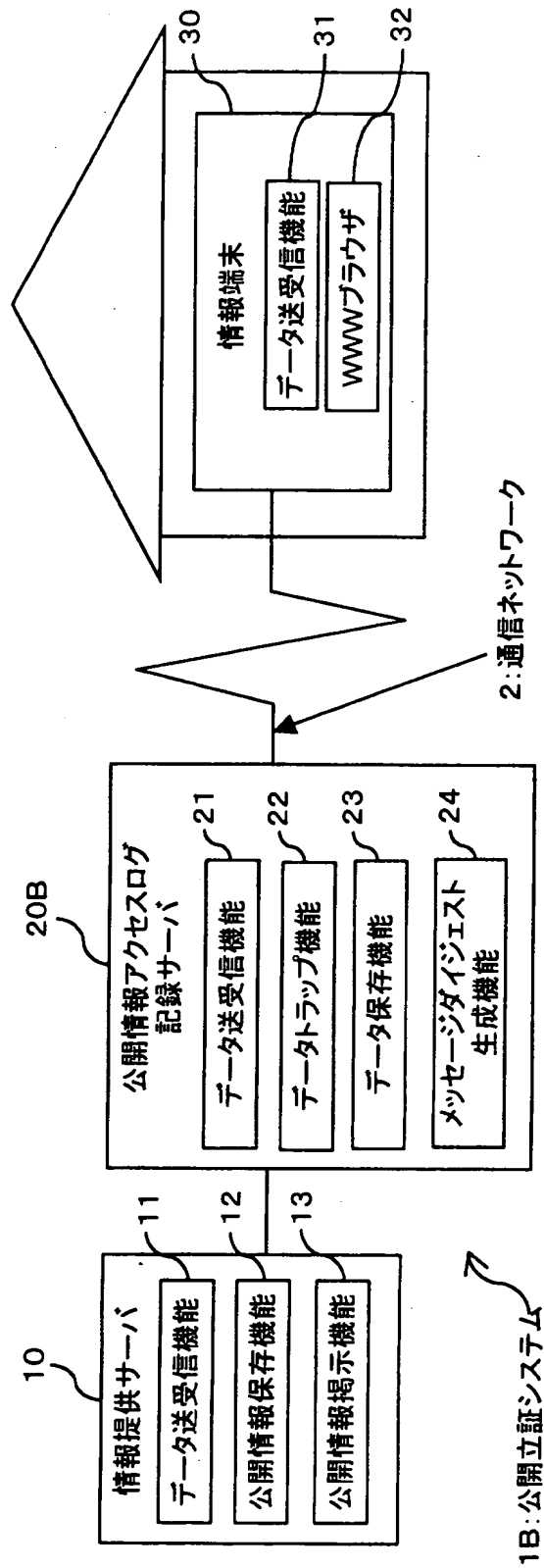
【図 2】

アクセス年月日
アクセス時刻
ドメイン情報
リモートホスト情報
ブラウザ名称情報
参照ディレクトリ情報

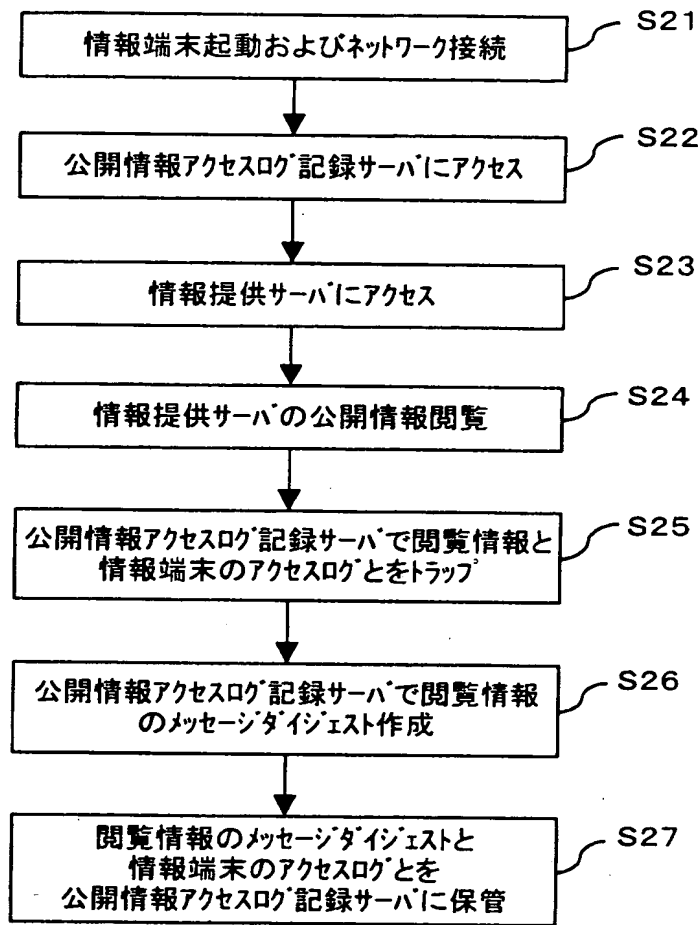
【図 3】



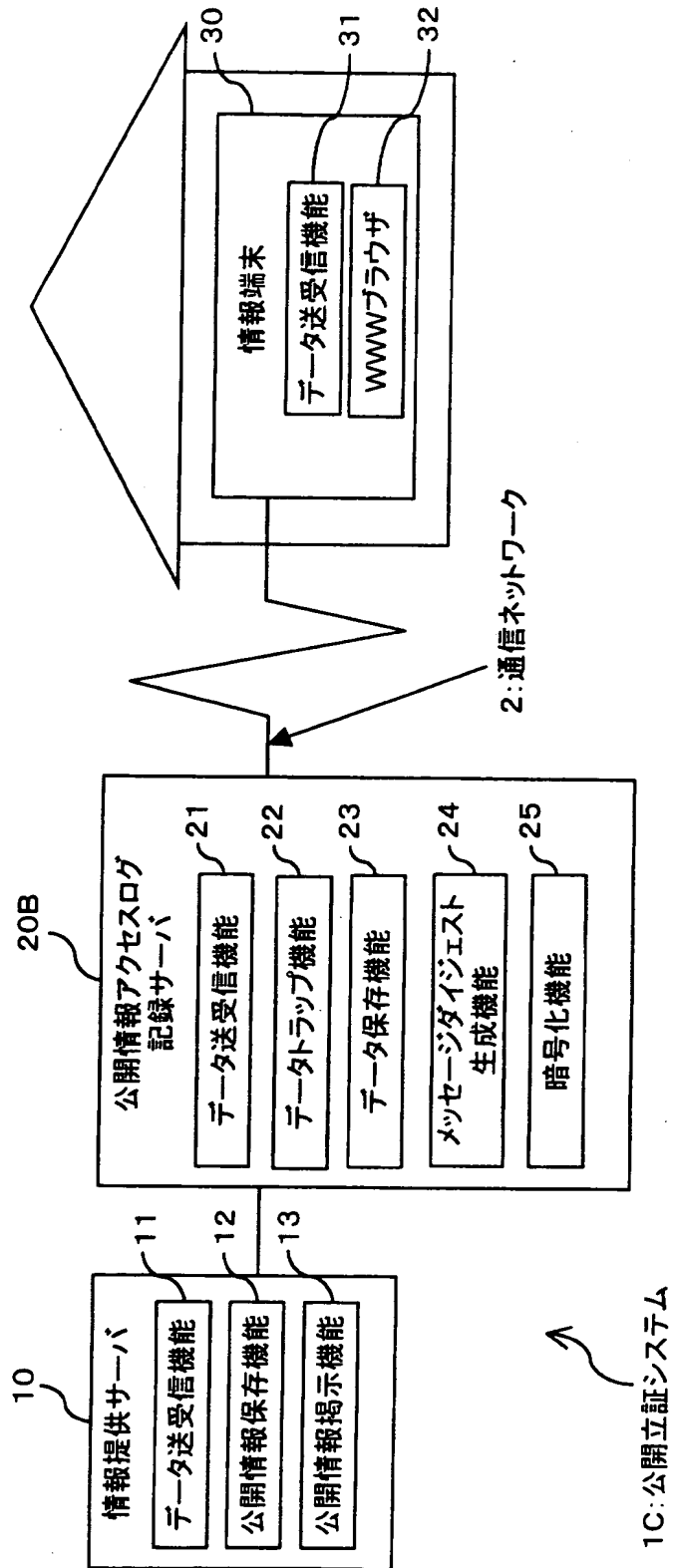
【図 4】



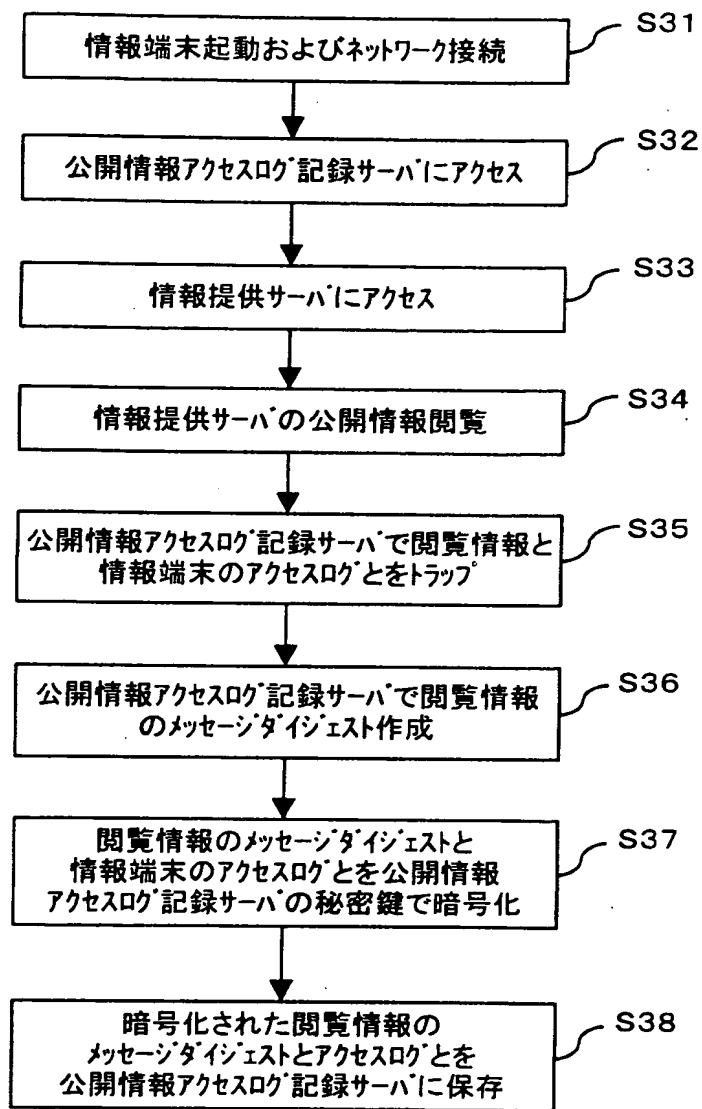
【図 5】



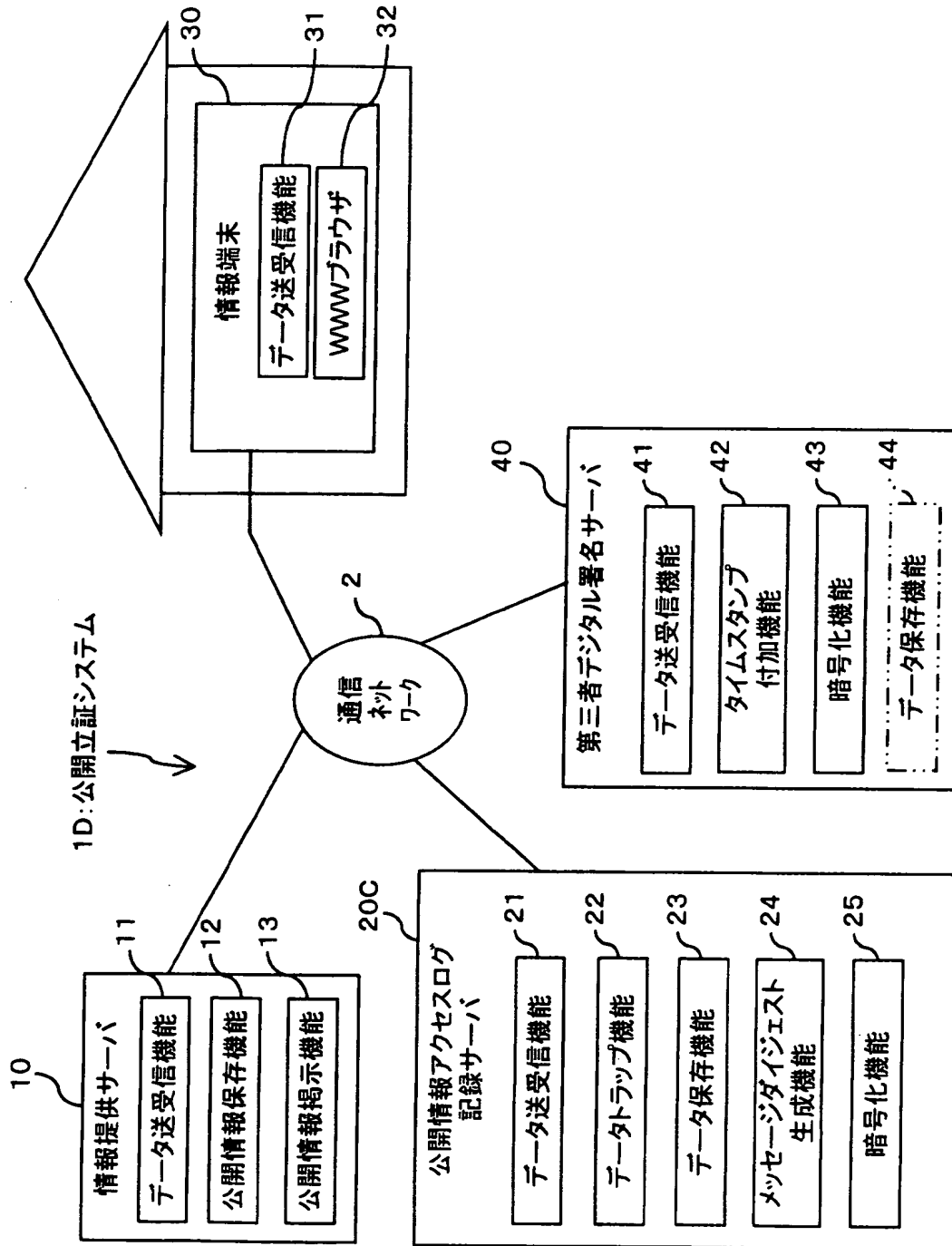
【図 6】



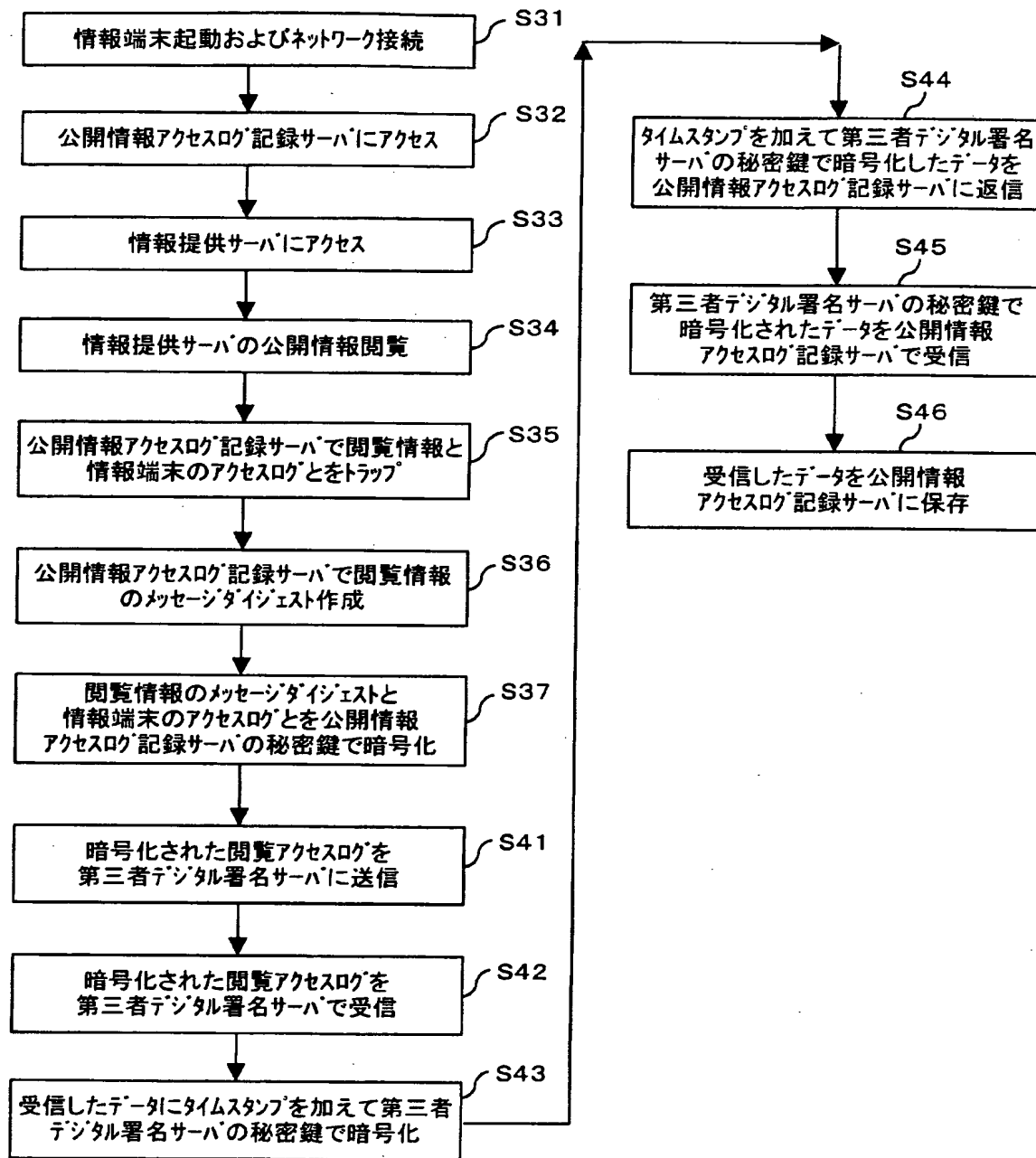
【図 7】



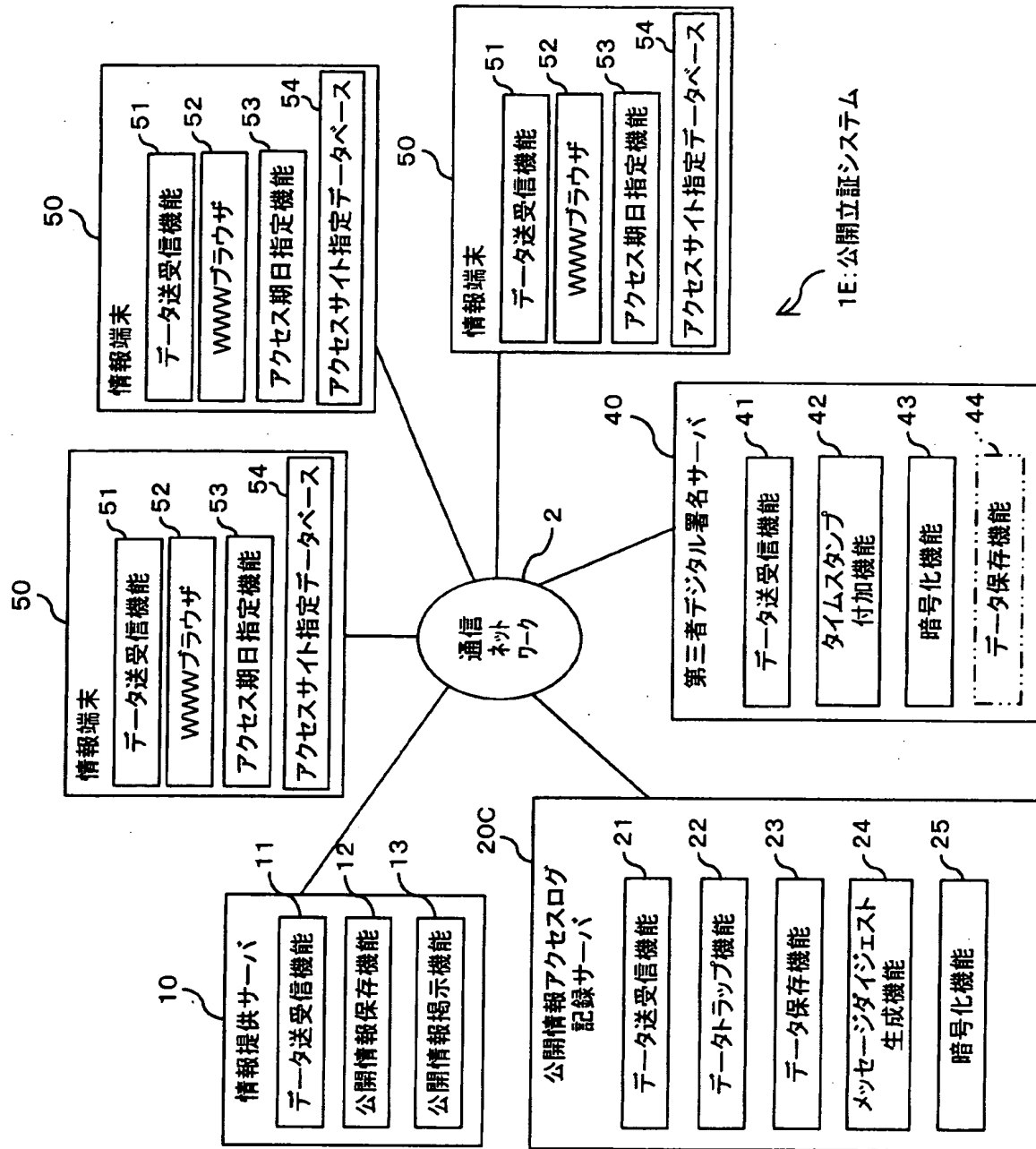
【図 8】



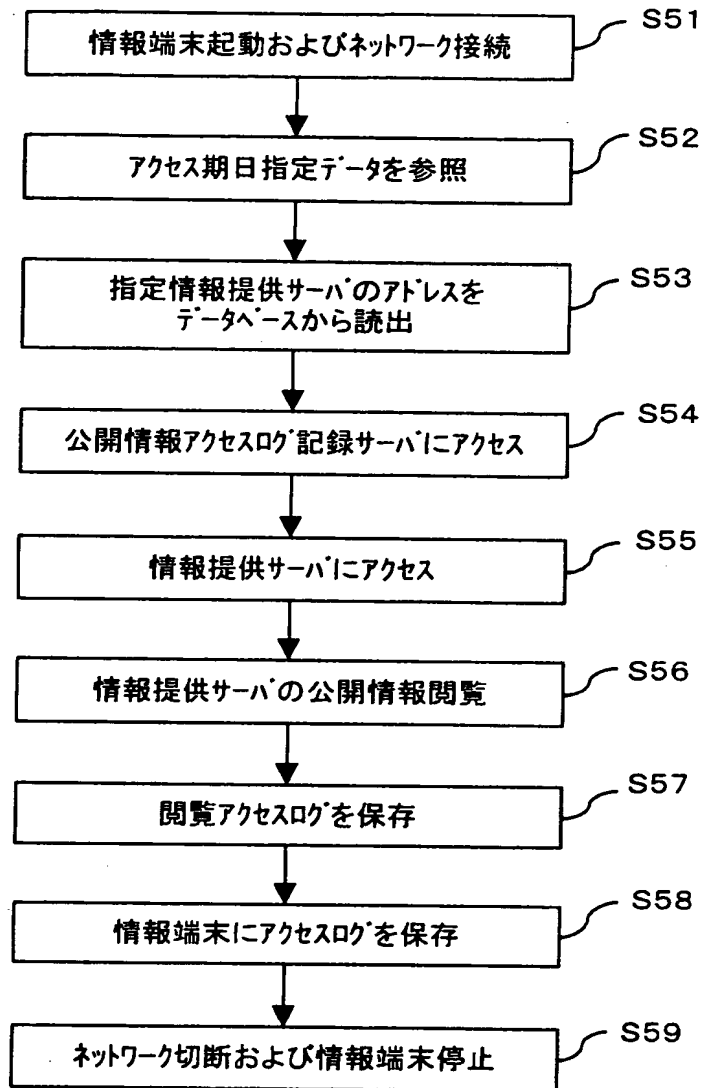
【図 9】



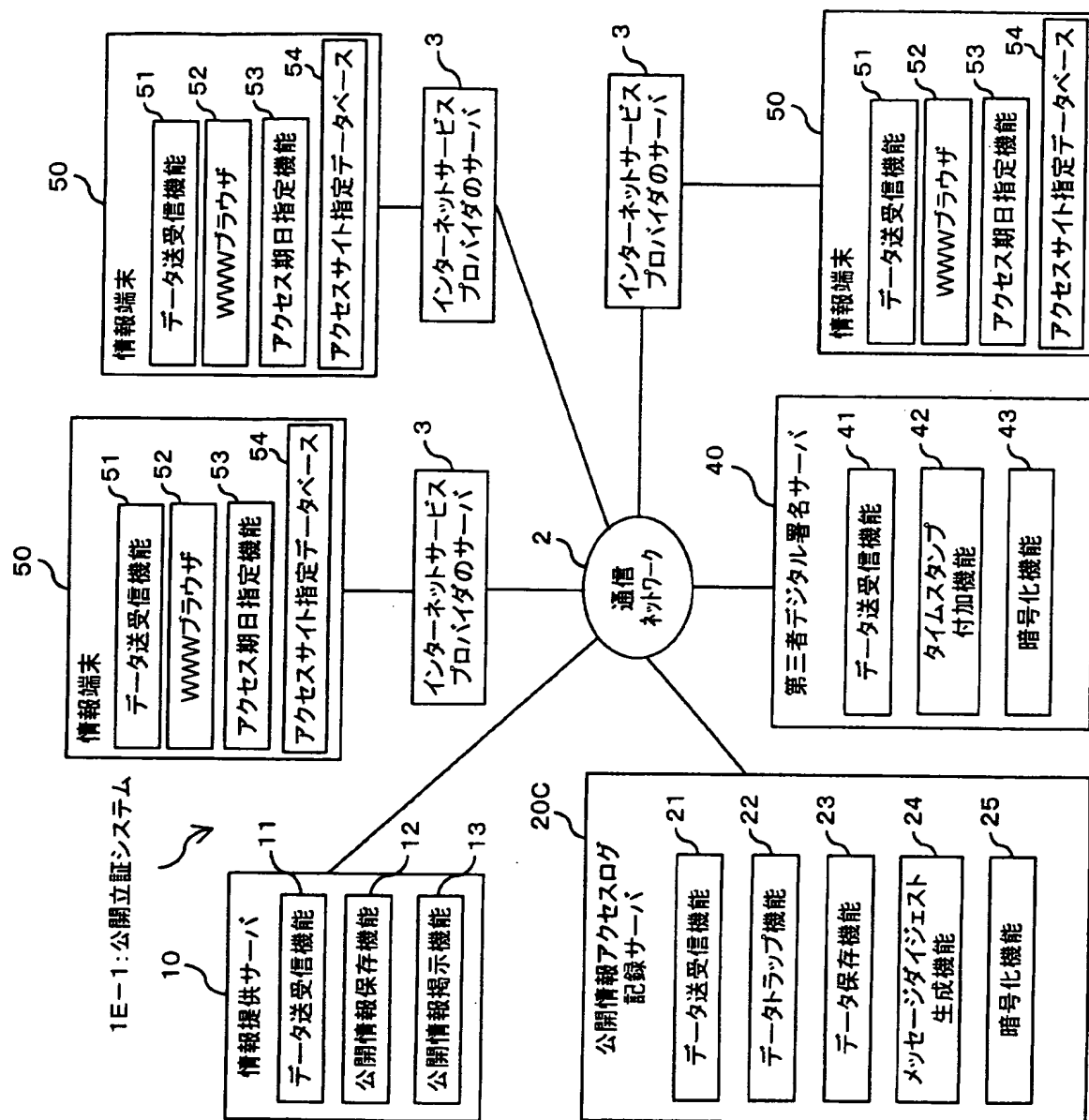
【図10】



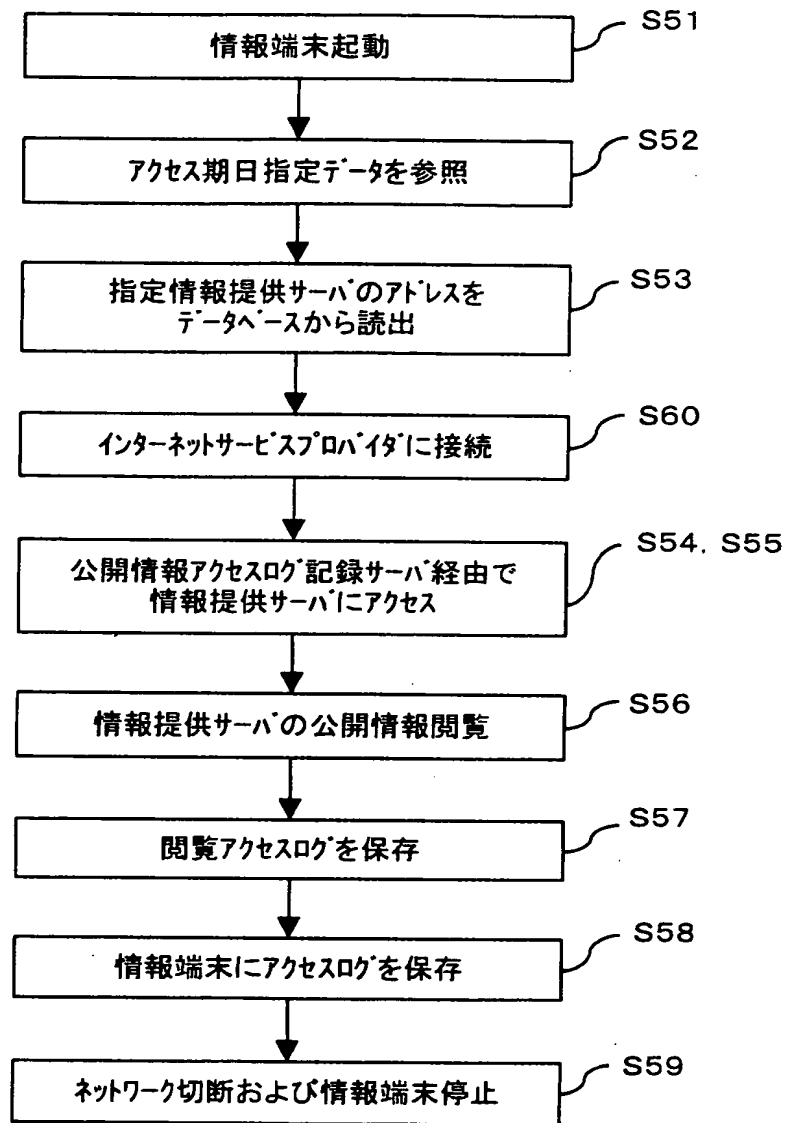
【図 1 1】



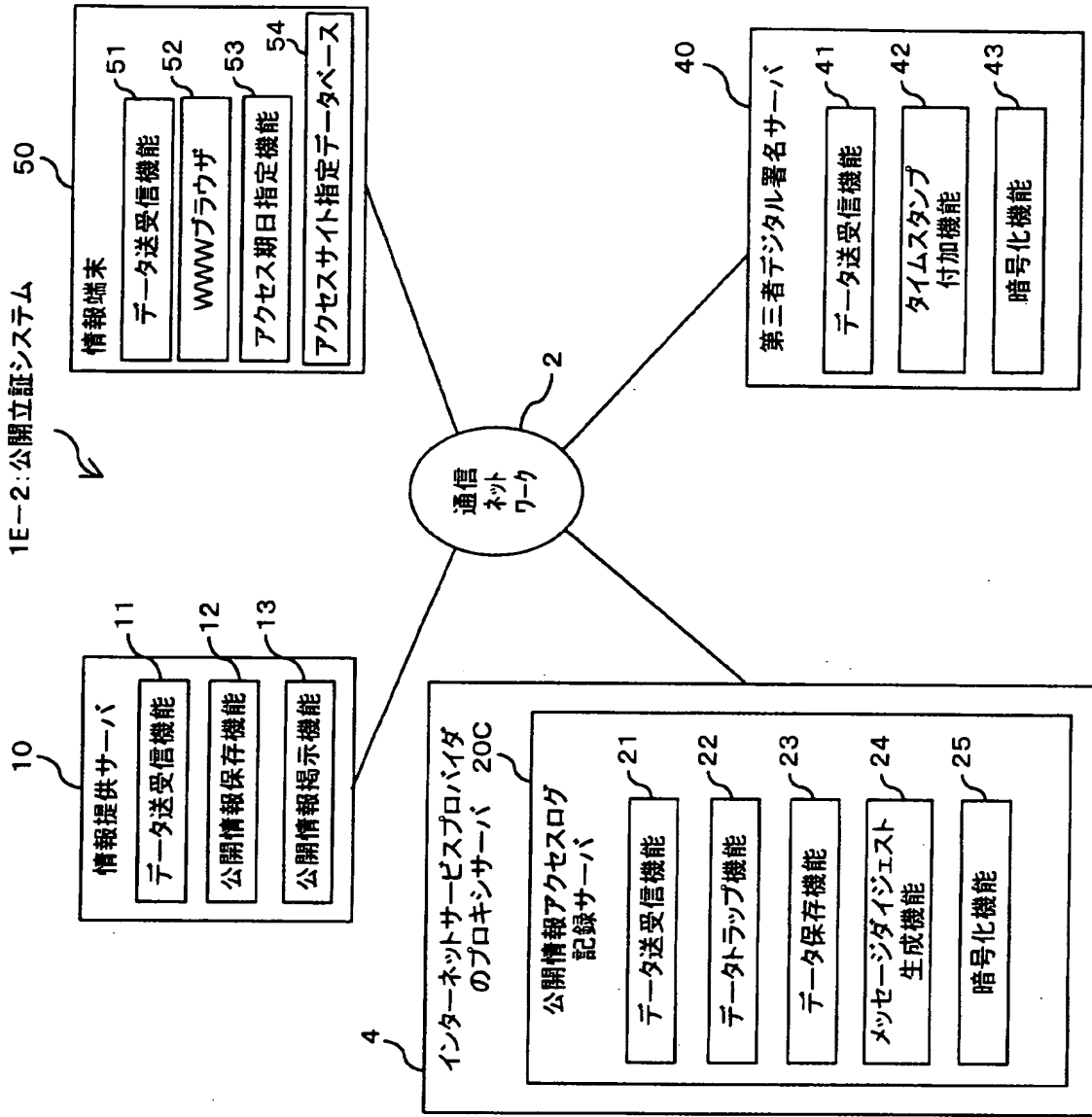
【図12】



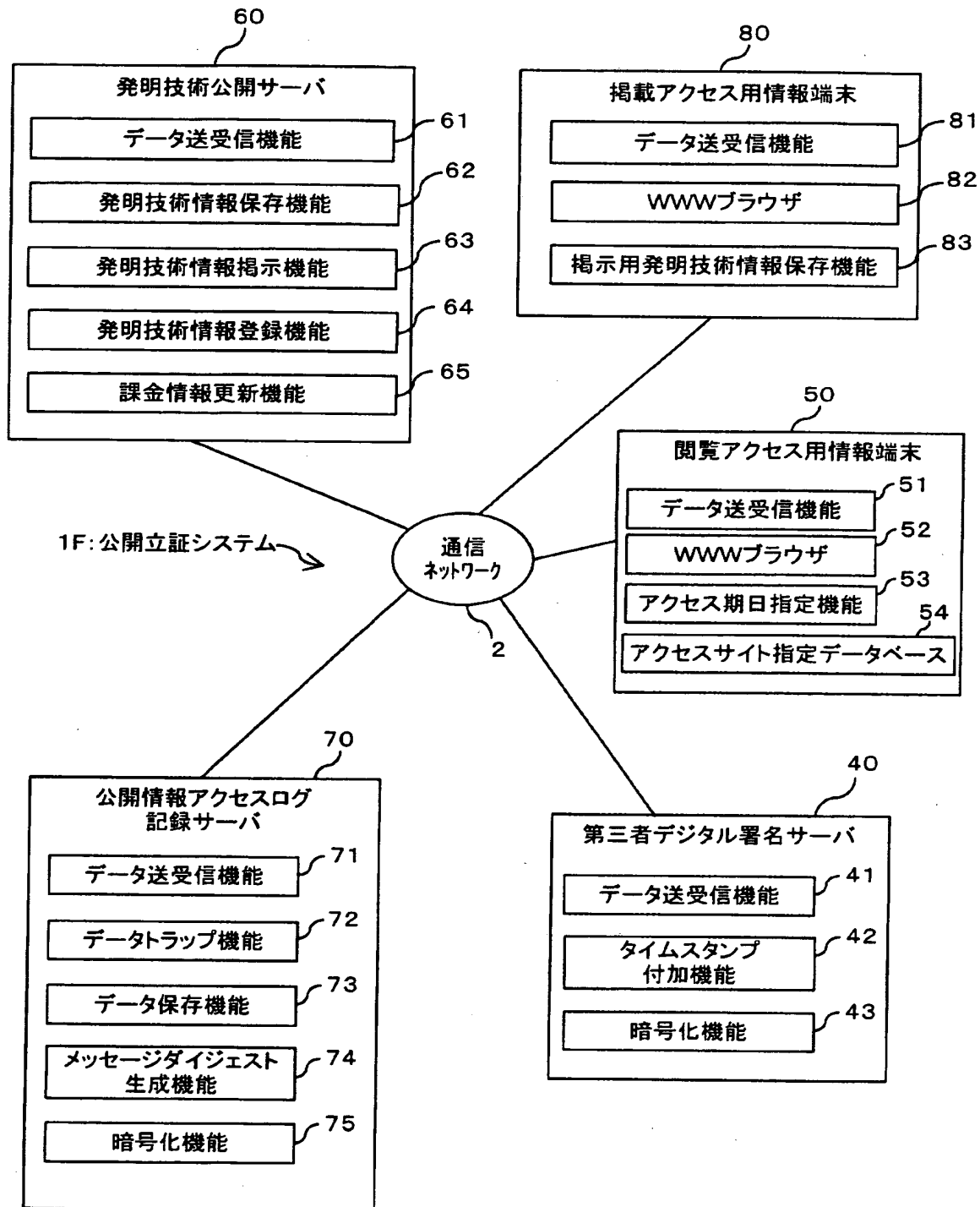
【図 1 3】



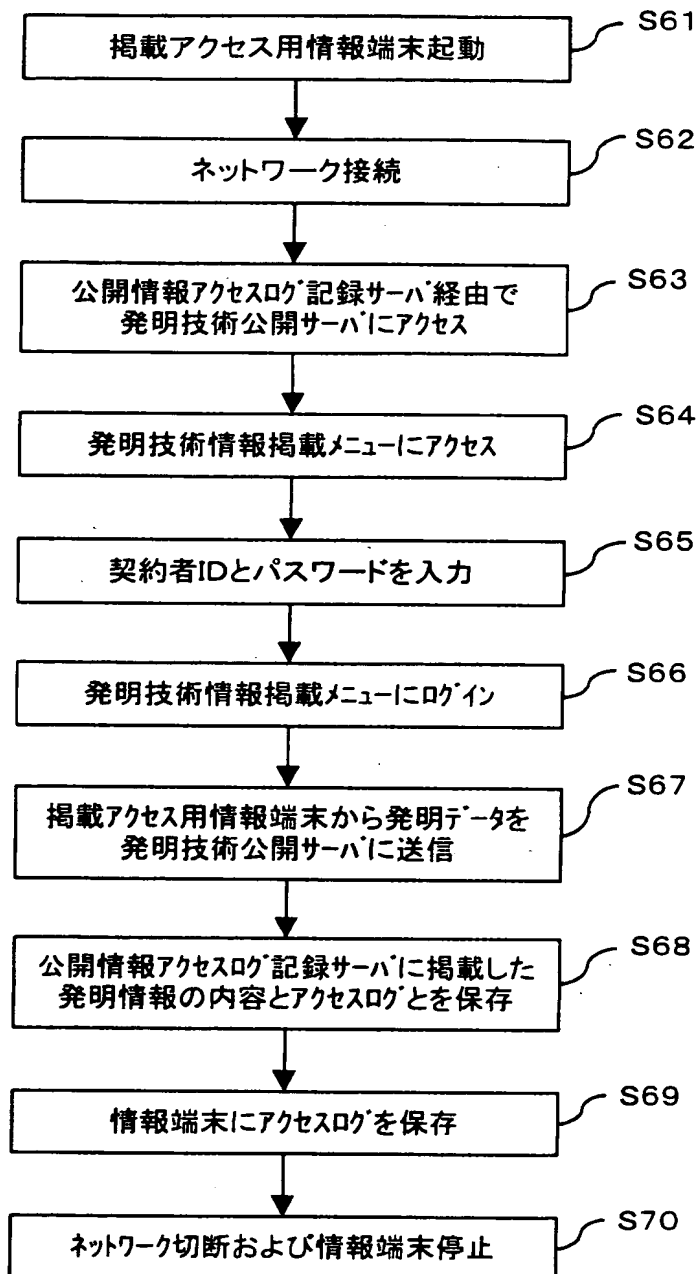
【図 14】



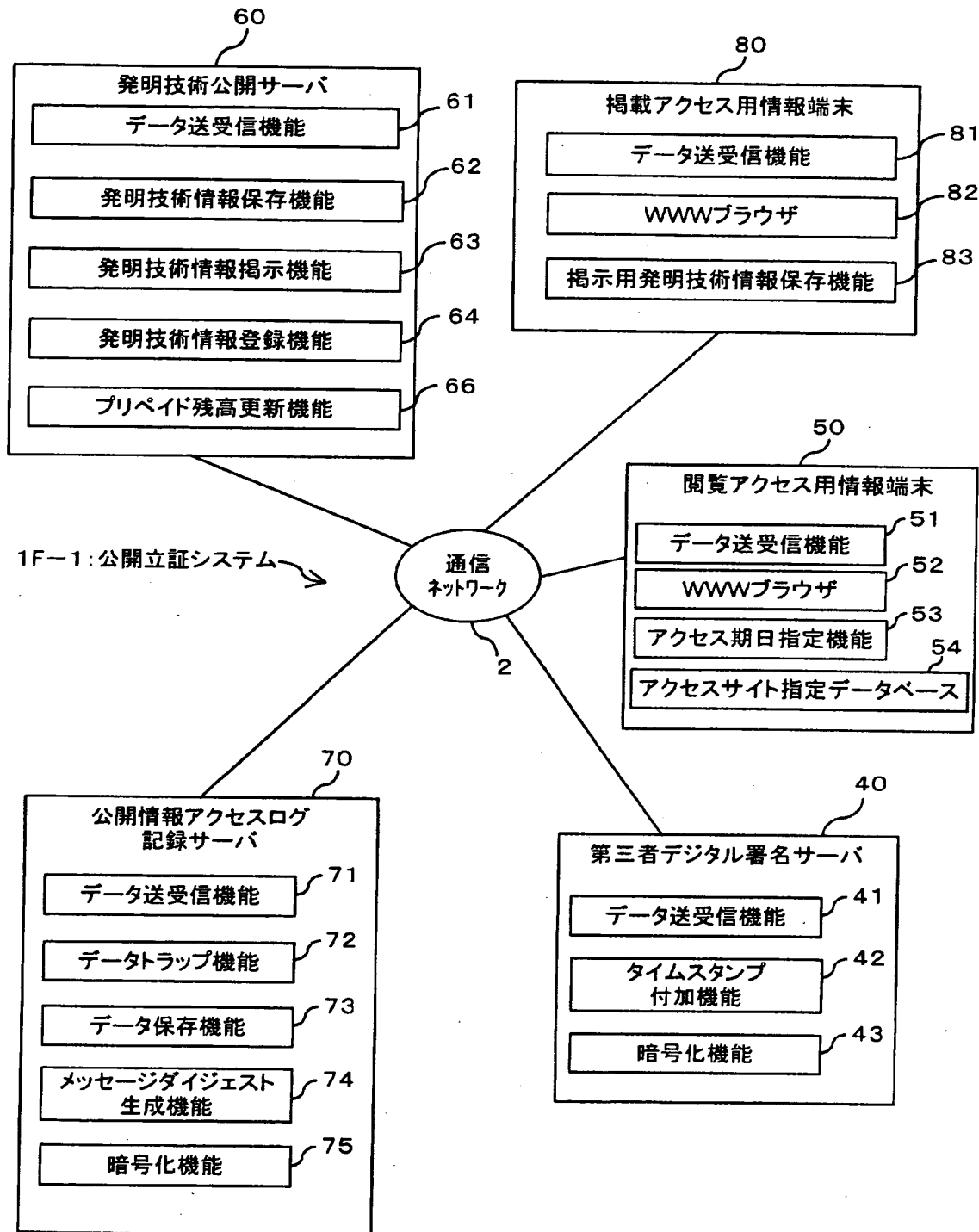
【図15】



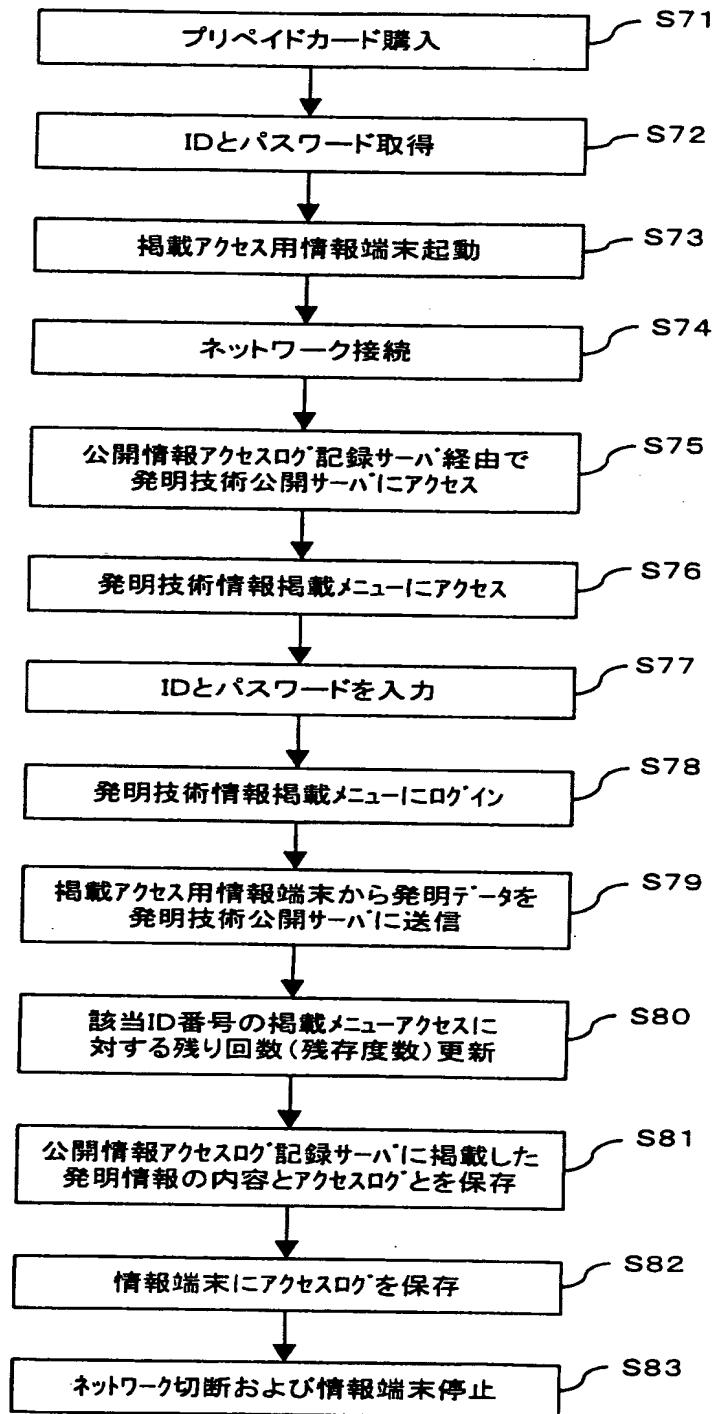
【図 1 6】



【図 17】



【図 18】



【書類名】 要約書

【要約】

【課題】 各種情報が電子データとしてネットワーク上において誰でもアクセス可能な状態にあったこと、即ち、その電子データがネットワーク上で掲示・公開されていたことを立証できるようにして、そのネットワーク上で掲示・公開された情報にも、印刷物や出版物と同様の証拠能力をもたせることを実現する。

【解決手段】 公開情報を保存する公開情報保存機能 1 2 と、公開情報を閲覧すべく通信ネットワーク 2 を介してアクセスしてきた情報端末 3 0 に対し公開情報を提供する公開情報掲示機能 1 3 とを有する情報提供サーバ 1 0 と、情報端末 3 0 により閲覧された公開情報とこの公開情報に対するアクセス日時とを閲覧アクセスログとして獲得するデータトラップ機能 2 2 と、このデータトラップ機能 2 2 によって獲得された閲覧アクセスログを保存するデータ保存機能 2 3 とを有する閲覧アクセスログ記録サーバ 2 0 A とをそなえて構成する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社